CS5438
Security and Privacy: Practice and Case Studies

$c = m^e \bmod n$

What's in Your Wallet?
3 February 2016

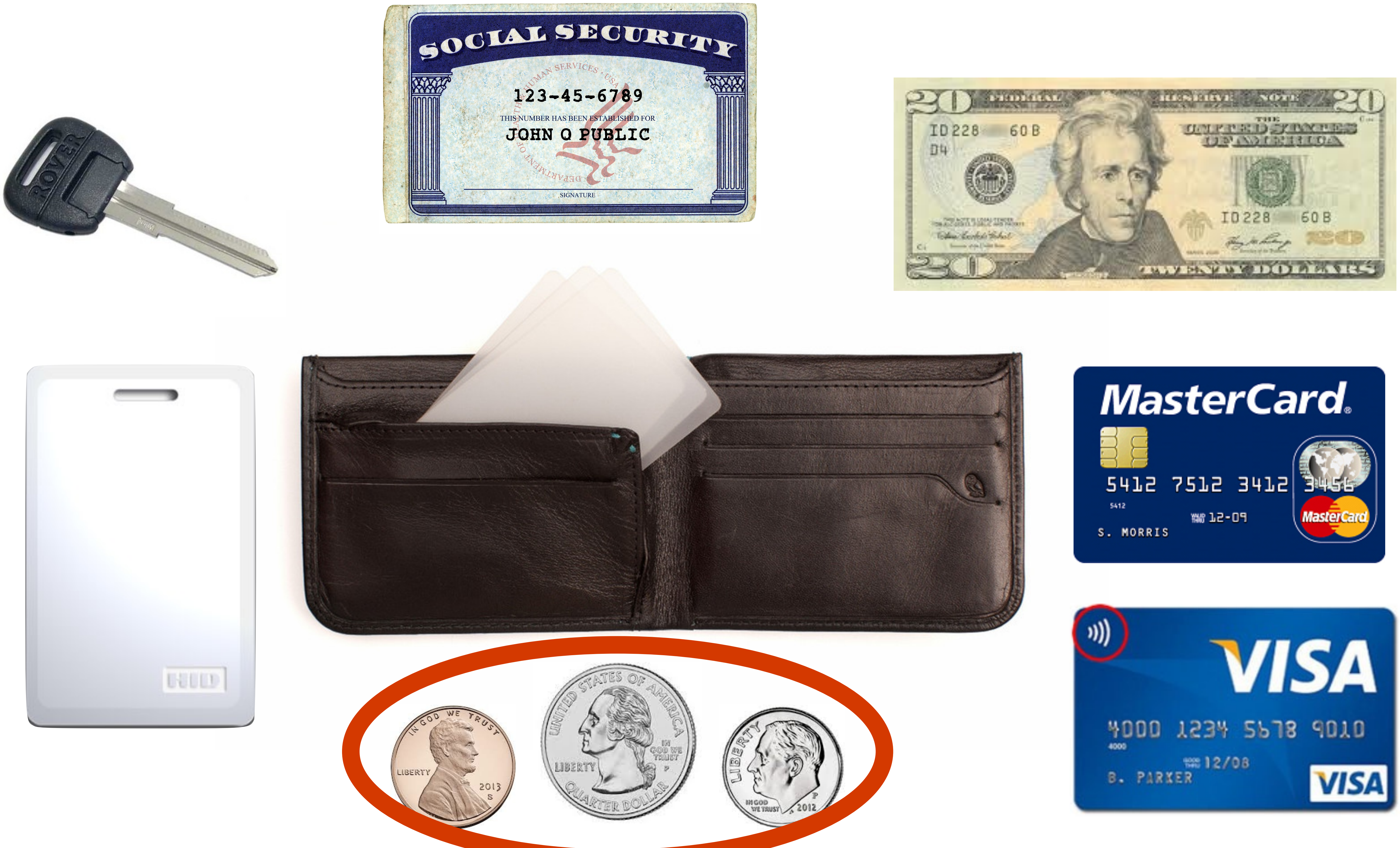
Instructors: Ari Juels and Vitaly Shmatikov
Spring 2016

“Some people can read *War and Peace* and come away thinking it's a simple adventure story. Others can read the ingredients on a chewing gum wrapper and unlock the secrets of the universe…”

–Lex Luthor, *Superman* (1978)

Anatomy of a wallet

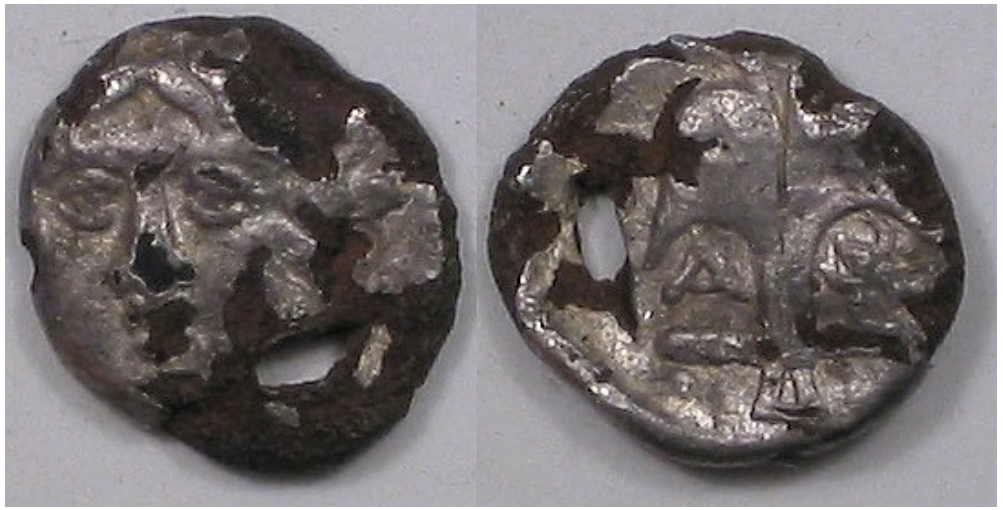
Anatomy of a wallet



Coins

- From last class, three key security mechanisms to deter forgery:
  1. Scarcity of material / resource
  2. Hard-to-reproduce signs / signatures
  3. (And the death penalty…)
- Helped reduce forgery, but forgers bypassed scarcity problem
- Suppose you've only got 1/10 ounce of silver, but you want to make a 1 ounce silver coin. What do you do?
- You coat 9/10 ounce of cheap metal in silver! Here's the result…

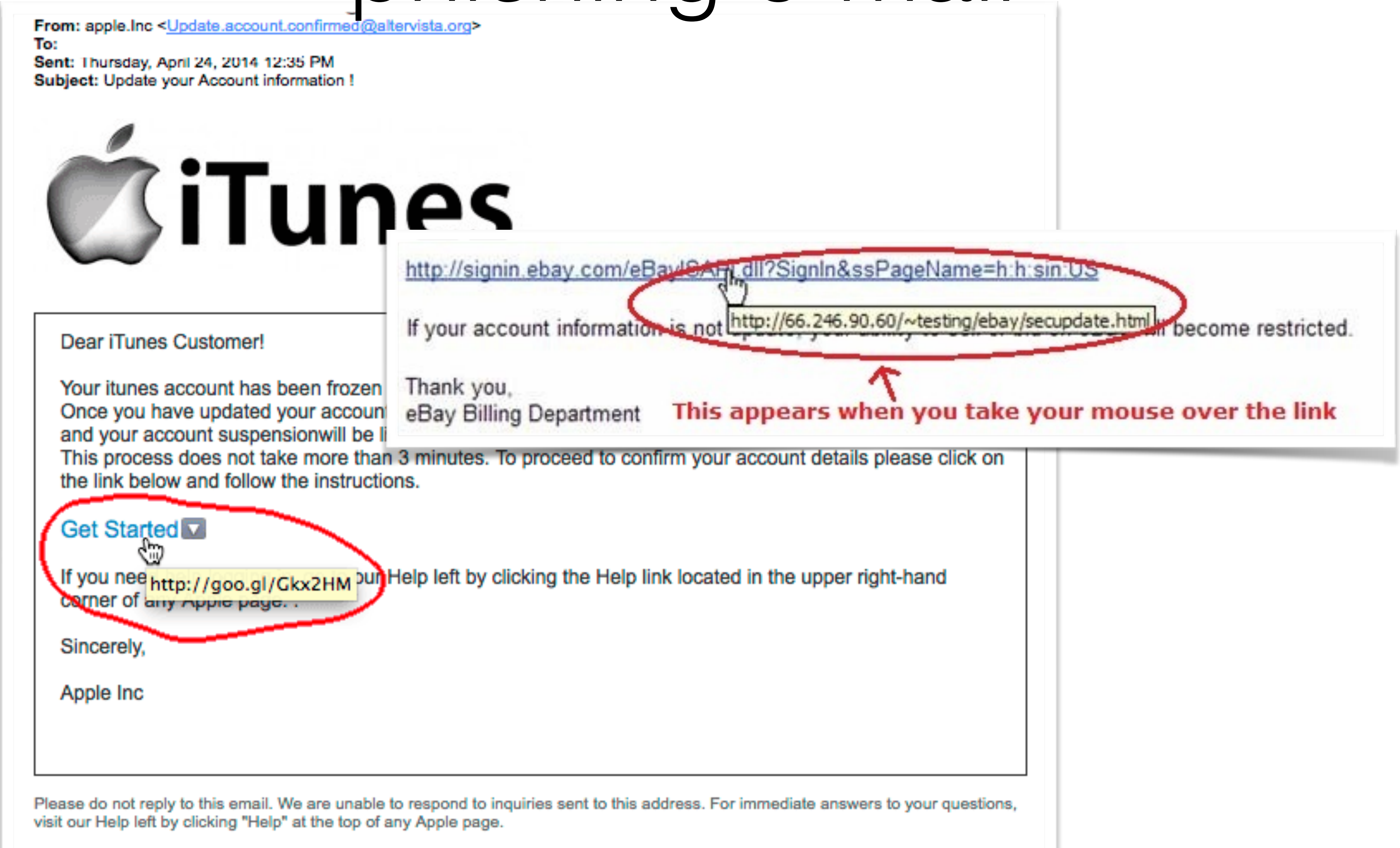
From the collection of Aaron Emigh. Lucania, Velia. 350-281 BC. Fourrée AR nomos (7.22g). SNG Copenhagen 1586.



From the collection of Aaron Emigh. Thrace, Apollonia Pontika. 450-400 BC. Fourrée AR diobol (0.87g).

fourées

Here’s the same trick in phishing e-mail



From: apple.Inc <Update.account.confirmed@altervista.org>
To:
Sent: Thursday, April 24, 2014 12:35 PM
Subject: Update your Account information !

Dear iTunes Customer!

Your itunes account has been frozen
Once you have updated your accoun
and your account suspensionwill be li
This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

http://goo.gl/Gkx2HM

If you nee our Help left by clicking the Help link located in the upper right-hand corner of

Sincerely,

Apple Inc

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

http://signin.ebay.com/eBayISAPI.dll?SignIn&ssPageName=h:h:sin:US

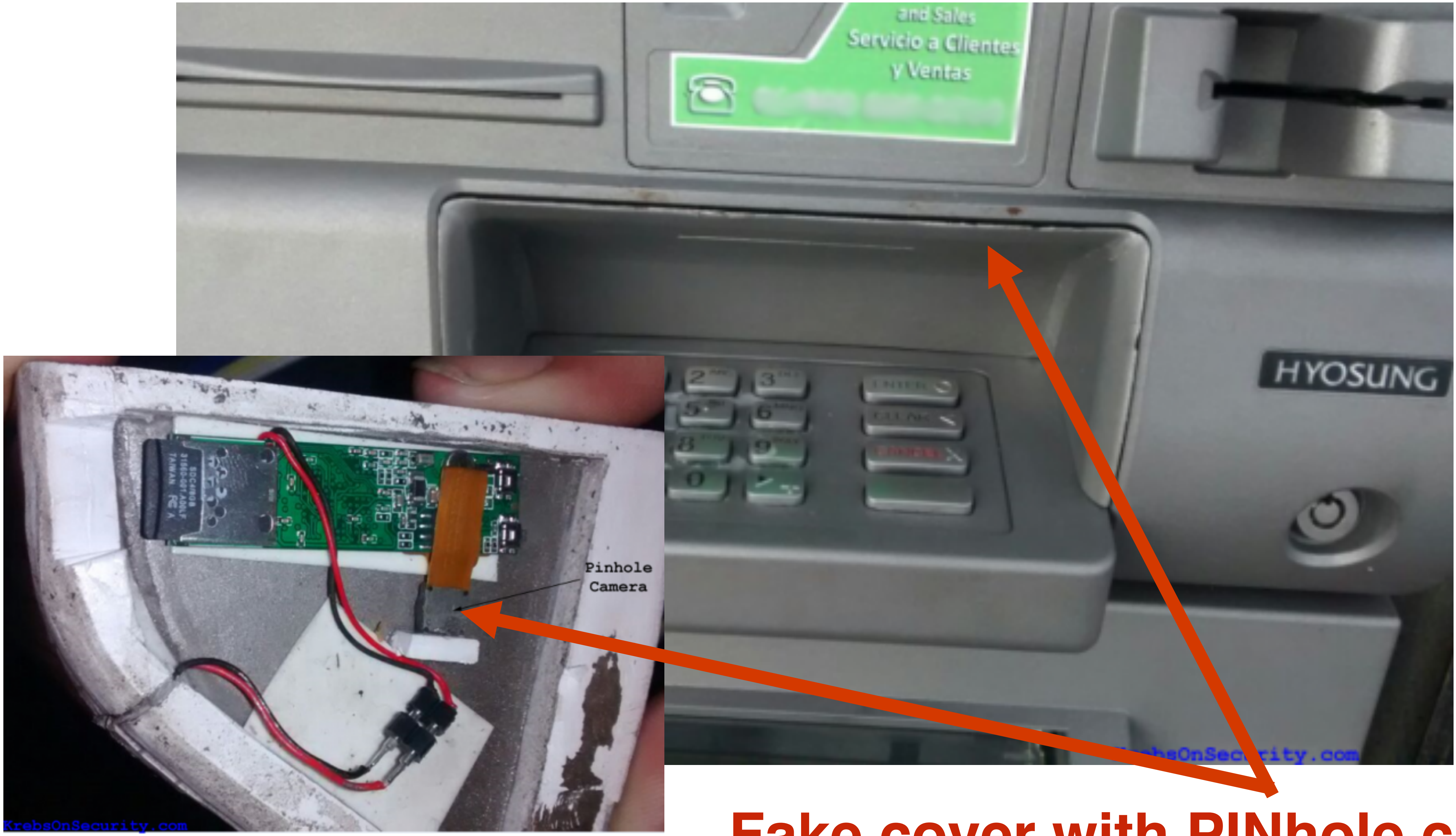
http://66.246.90.60/~testing/ebay/secupdate.html

If your account information is not become restricted.

Thank you,
eBay Billing Department

This appears when you take your mouse over the link

And in an ATM PIN capture device

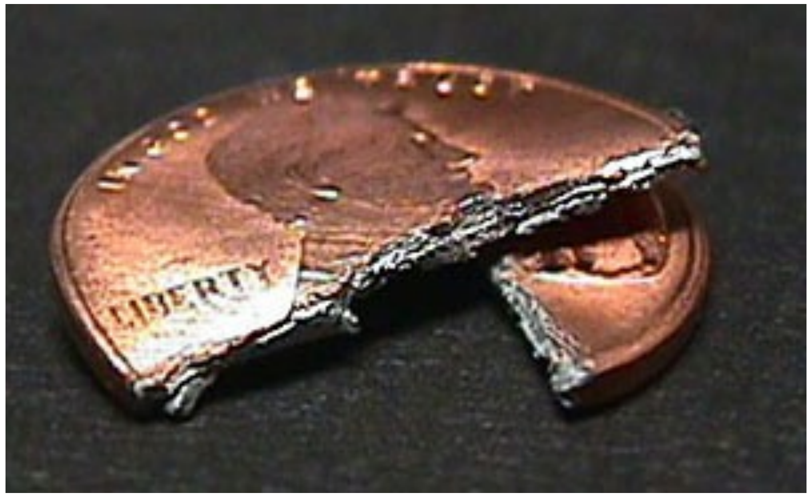


Fake cover with PINhole camera

[Source: Krebs on Security, 15 July 2015]

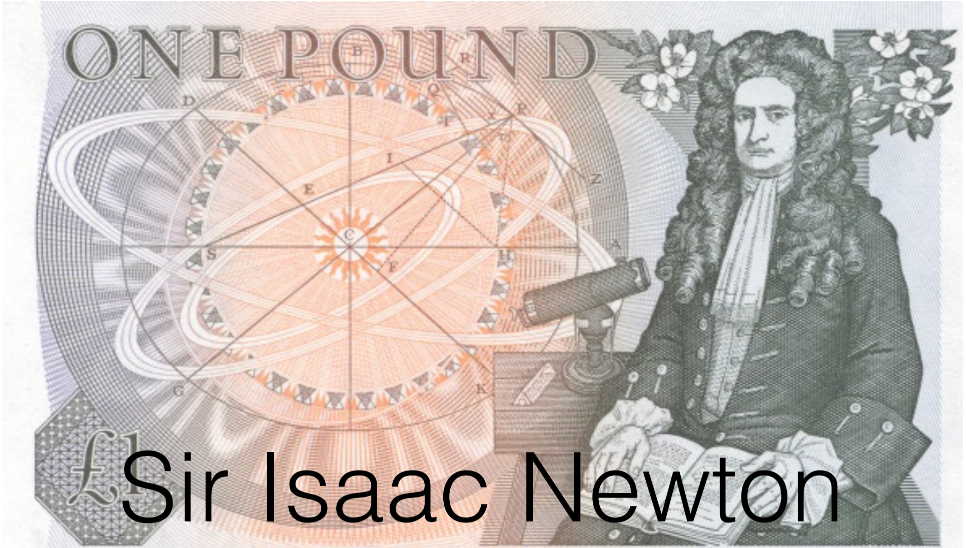
Same trick also used for benign purposes

The penny is a U.S. government issue fourée!



Authentic coins could still be tampered with…

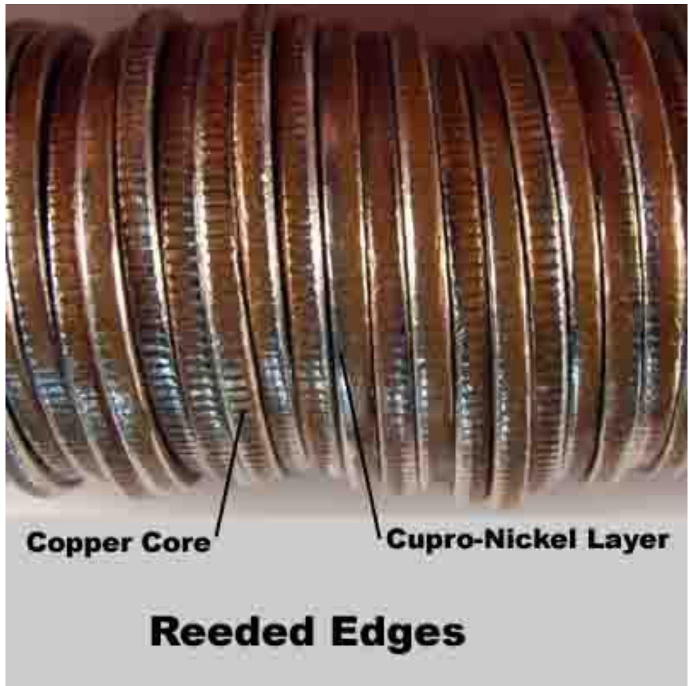
- Clipping and shaving affected their physical **integrity**.
- It got so bad, that in England in 1695, one survey showed coins contained just over half their prescribed weight!
- The solution?
  - Decorated or reeded edges
- Great Recoinage of 1696 reminted all currency with decorated edges; overseen by Warden of the Mint…



Sir Isaac Newton

Coins today still have reeded edges

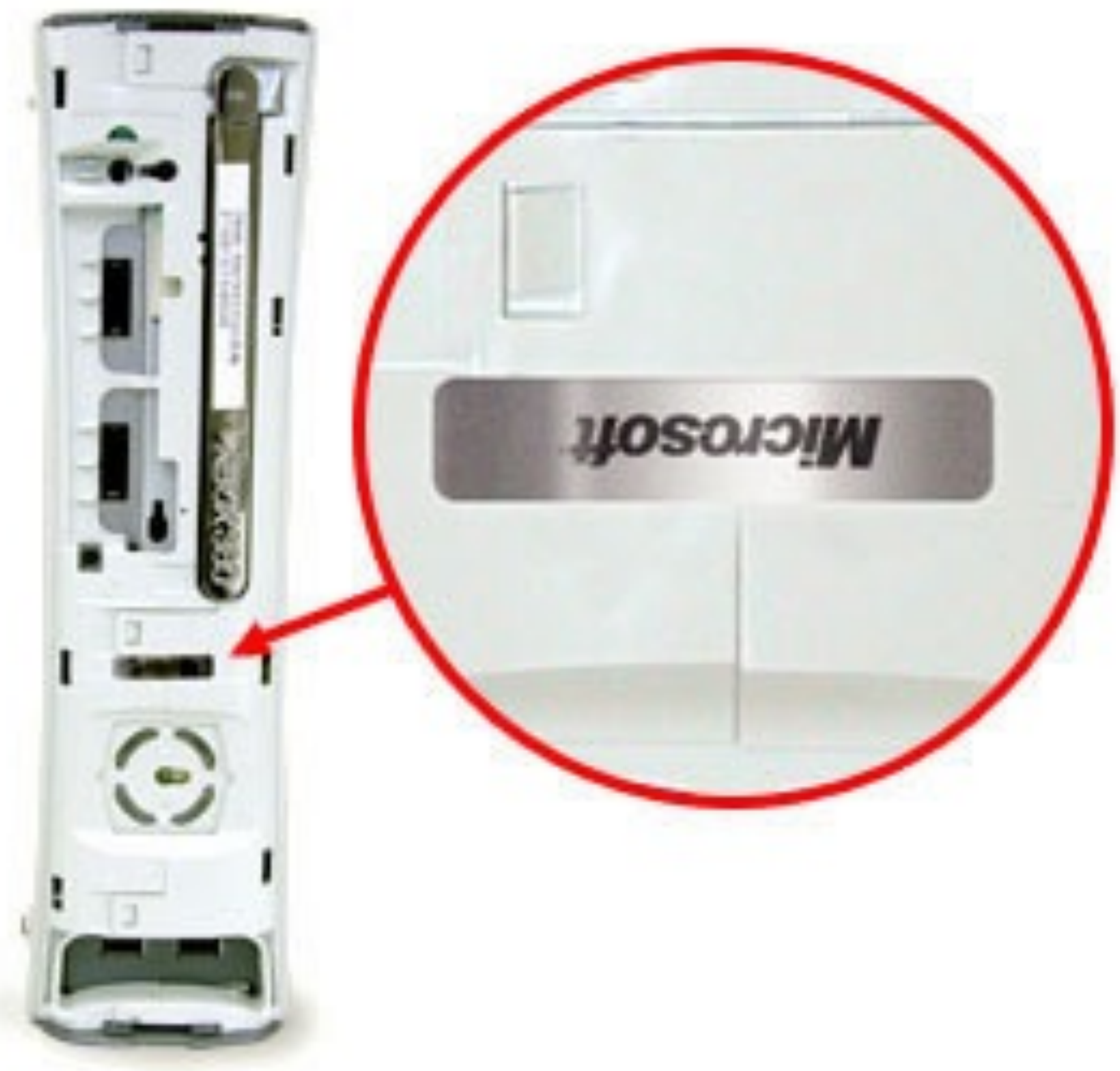
But they’re no longer useful, just decorative.



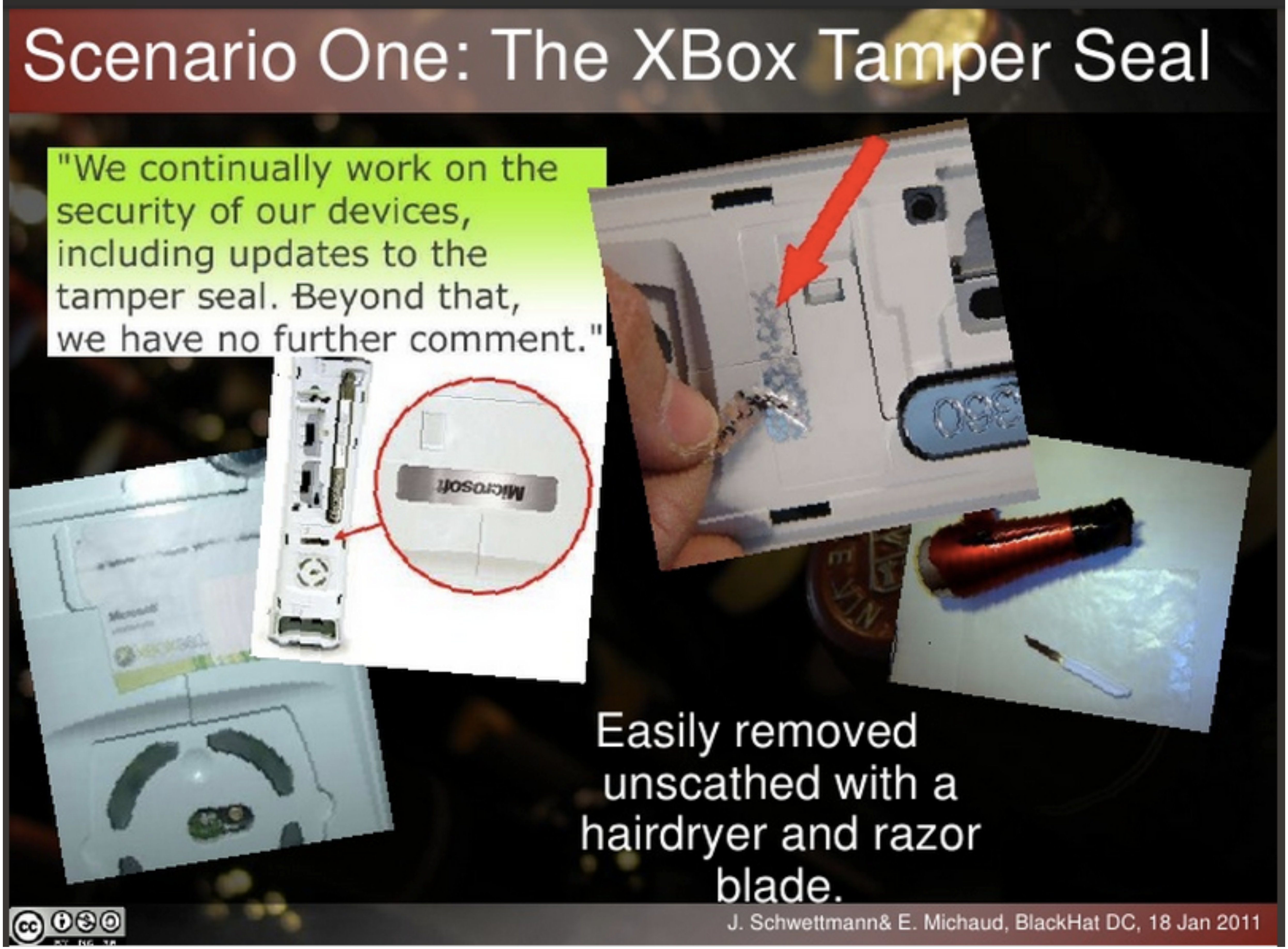
Reeding is an early example of “tamper evidence”

- Today, a similar requirement arises in the protection of cryptographic “modules”—hardware or software components that perform cryptography. (E.g., smartcards.)
- Federal Information Processing Standard (FIPS)140-2 Level 2 (and above) requires tamper evidence.
- It’s also common in consumer products.

Such as the Xbox



Security goal: Prevent undetected mods



Scenario One: The XBox Tamper Seal

"We continually work on the security of our devices, including updates to the tamper seal. Beyond that, we have no further comment."

Easily removed unscathed with a hairdryer and razor blade.

J. Schwettmann& E. Michaud, BlackHat DC, 18 Jan 2011

From J. Schwettmann and E. Michaud, “How To Steal A Nuclear Bomb, Without Voiding You

Credit cards too have holograms

- “Hard-to-duplicate” sign / signature of coinage in 20th century
  - Introduced in credit cards by Mastercard in 1982
- Increasingly easy to duplicate
  - A police expert estimated already in early 1990s more than 100 forgers in China capable of producing authentic-looking holograms.
  - In 2014, fakeplastic.net raided by FBI and USPS in NJ; had tens of thousands holograms for credit cards and drivers licenses.

Anatomy of a wallet

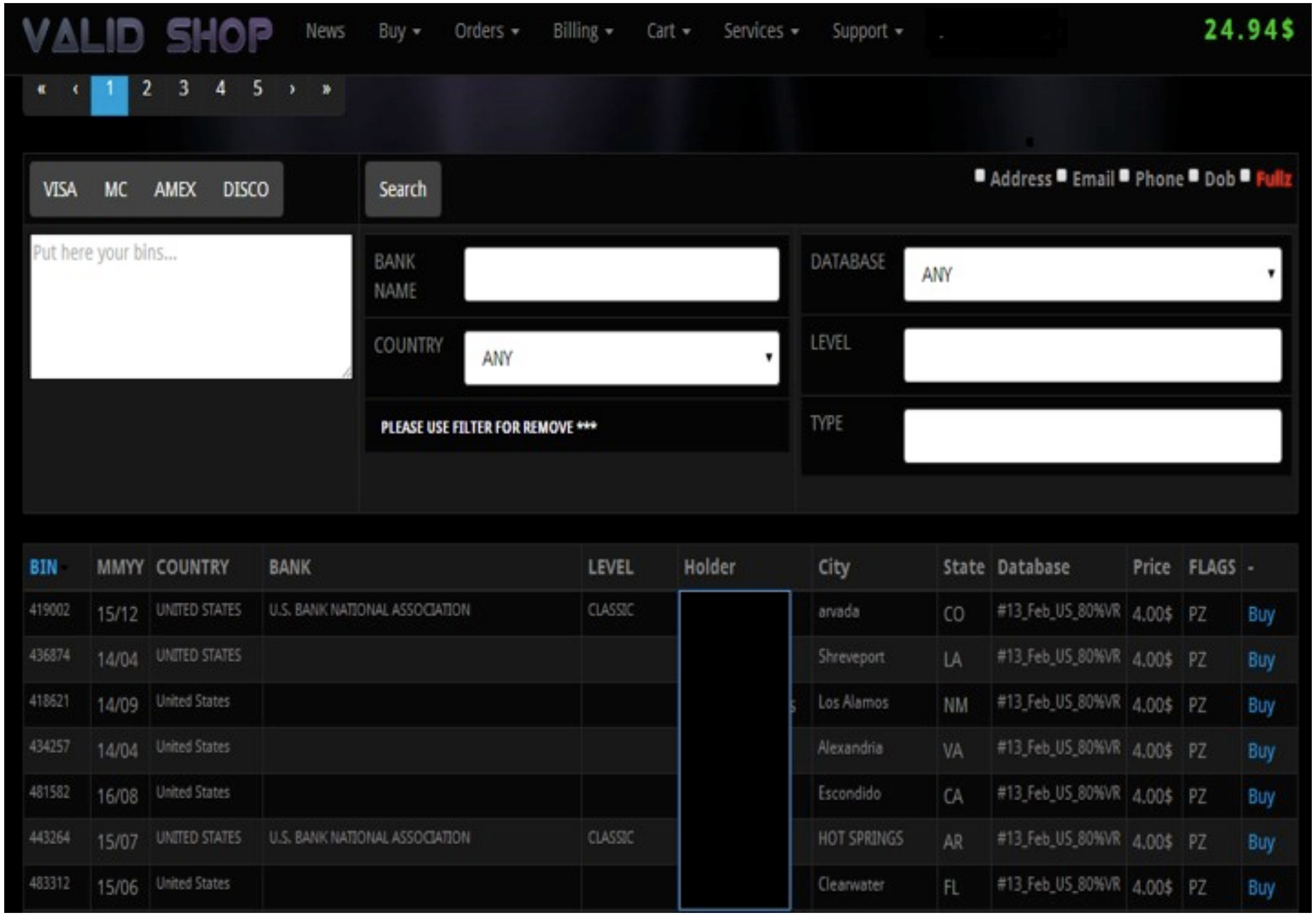
Credit card fraud is a massive problem

- Businesses worldwide lost $14+ billion in 2013
- U.S. accounted for 51% of worldwide credit card fraud in 2013 (but only 1/4 of payments)
- Whole underworld ecosystem for theft and sale of credit-card numbers
  - Well-developed international business!

ValidShop.su

"Amazon of the cybercrime economy"

- "The shopping experience is great if you are a bad guy."
    - F. Y. Rashid, SecurityWatch, "RSAC: Buying, Selling Stolen Credit Cards Online," 28 Feb. 2014
- Instant validity check; refund for invalid cards
- Payment in Bitcoin



BANK NAME

COUNTRY: ANY

DATABASE: ANY

LEVEL

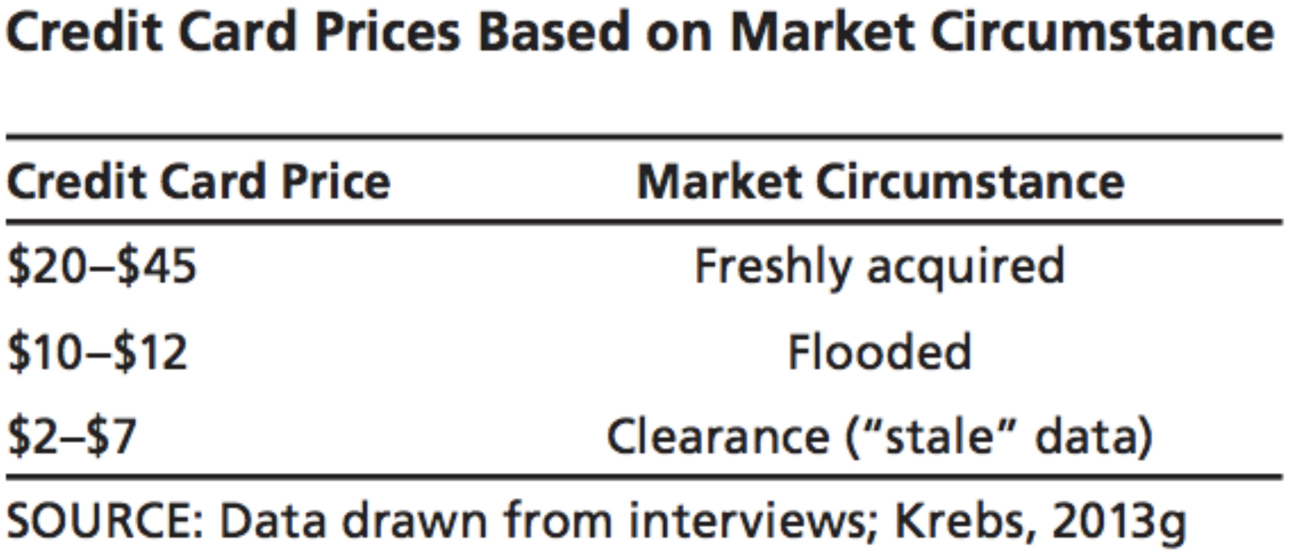
TYPE

PLEASE USE FILTER FOR REMOVE ***

BIN	MMYY	COUNTRY	BANK	LEVEL	Holder	City	State	Database	Price	FLAGS	-
419002	15/12	UNITED STATES	U.S. BANK NATIONAL ASSOCIATION	CLASSIC	[redacted]	arvada	CO	#13_Feb_US_80%VR	4.00$	PZ	Buy
436874	14/04	UNITED STATES			[redacted]	Shreveport	LA	#13_Feb_US_80%VR	4.00$	PZ	Buy
418621	14/09	United States			[redacted]	Los Alamos	NM	#13_Feb_US_80%VR	4.00$	PZ	Buy
434257	14/04	United States			[redacted]	Alexandria	VA	#13_Feb_US_80%VR	4.00$	PZ	Buy
481582	16/08	United States			[redacted]	Escondido	CA	#13_Feb_US_80%VR	4.00$	PZ	Buy
443264	15/07	UNITED STATES	U.S. BANK NATIONAL ASSOCIATION	CLASSIC	[redacted]	HOT SPRINGS	AR	#13_Feb_US_80%VR	4.00$	PZ	Buy
483312	15/06	United States			[redacted]	Clearwater	FL	#13_Feb_US_80%VR	4.00$	PZ	Buy

The market for credit card fraud

- How much do stolen cards cost?
- Example: Target breach in late 2013
  - Stolen Target cards originally $20 -$135 apiece
  - Prices dropped rapidly due to market flooding
  - Under normal circumstances…



Credit Card Prices Based on Market Circumstance

Credit Card Price	Market Circumstance
$20–$45	Freshly acquired
$10–$12	Flooded
$2–$7	Clearance ("stale" data)

SOURCE: Data drawn from interviews; Krebs, 2013g

Source: L. Ablon, M.C. Libicki, A. A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* RAND Corporation. 2014.

What can issuers and associations do?

- Once criminal has card number (and CVV), is the game up?
- Issuers (your bank) have rich transaction information:
  - Purchase type (groceries or a luxury handbag?)
  - Purchase price
  - Purchase time and location
  - Merchant identity
- They model consumer behavior and look for **anomalies**, i.e., *deviations from normal / good behavior*, e.g.,:
  - Use of cards in atypical / never visit places
  - Purchase of unusual items
- We'll talk these models in a later class and uses in detecting stolen passwords, compromised systems, etc.

Also…

- Banks also model and look for **criminal behavior**, e.g.,
  - Criminals test stolen cards unobserved with small transactions, e.g., buying gas… or making small donation to charity online
- When bank asks you to confirm a legitimate transaction, their anomaly detection has misfired (false positive).
- Companies and law enforcement monitor criminals
- Sometimes they do surprising things!
  - E.g., In 2006, DarkMarket was a major site for stolen credit cards
  - A primary admin was called Master Splyntr
  - Master Splyntr was… FBI agent Keith Mularski
  - Thanks to Mularski, 60 arrests worldwide
  - Classic counterintelligence…

What’s that chip?

- The EMV (Europay, MasterCard, and Visa) protocol is a smartcard-based credit-card standard
  - Also known as “Chip and PIN” with PIN option
  - Has tamper resistance
  - Implements cryptographic authentication
- Common in Europe; over 2+ billion cards circulating worldwide (2014).
- Increasing use in U.S…
- Merchants in U.S. were liable for fraud as of Oct. 2015 if they lack EMV-enabled payment terminal

What’s that chip?

- Tamper-resistant hardware and cryptography should result in lower fraud rates, right?
- Yes and no.
- In France, for instance, fraud rates increased (!) after introduction of EMV.
- Why? Criminals exploited a loophole:
  - Face-to-face fraud rate (2009) was 0.01%. It dropped under EMV.
  - “Card-not-present” rates (2009) were 0.26% (domestic) and 1.35% (cross-border). They rose under EMV.

What’s that chip?

- Banks and regulators rejecting in-store consumer fraud claims because “Chip and PIN is secure”
- “Chip and PIN is Broken” paper (Murdoch et al., 2010) showed flaws in U.K. system
  - Fraudster could use card without knowing PIN
- What will happen in the U.S.?
  - Lots of legacy infrastructure
  - Online purchases increasing
  - So we shall see!

Anatomy of a wallet

Tap-and-go credit cards

- Cards with chips that transmit credit card information via short-range radio
- Wireless microchips often called Radio-Frequency IDentification (RFID)
- Passive, meaning power comes from reader
- Read range on the order of 10cm to 30cm
- 100 million circulating (2012)

How does it work?

- Consumer authorizes payment by tapping card on terminal
  - Or tapping an (NFC-enabled) phone, e.g., Apple Pay
- Processing happens on the back end, as for ordinary card

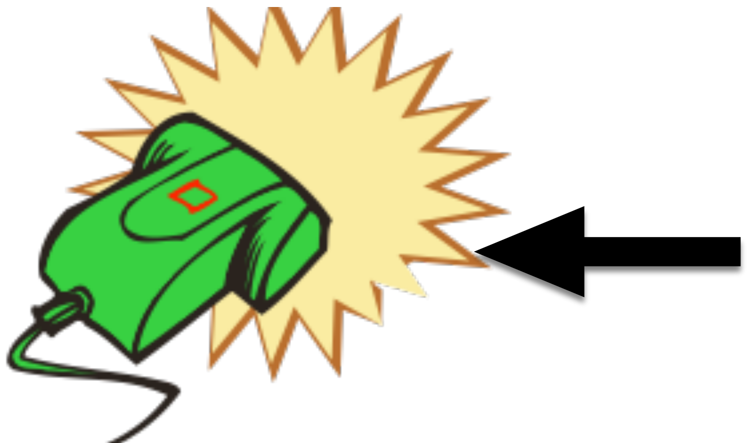
What could go wrong?

- Theme in this class…
  - Security as afterthought
- In 2007,
  - Some first-generation tap-and-go cards simply emitted (ISO 7813) magstripe data.
  - Some tap-and-go cards emitted cardholder names.
    - Why is this bad?
- Vulnerable to tracking
- Vulnerable to “skimming"…

S. Parker
Card number
4000 1234 5678 9010
Exp: 12/08
CVV: 977

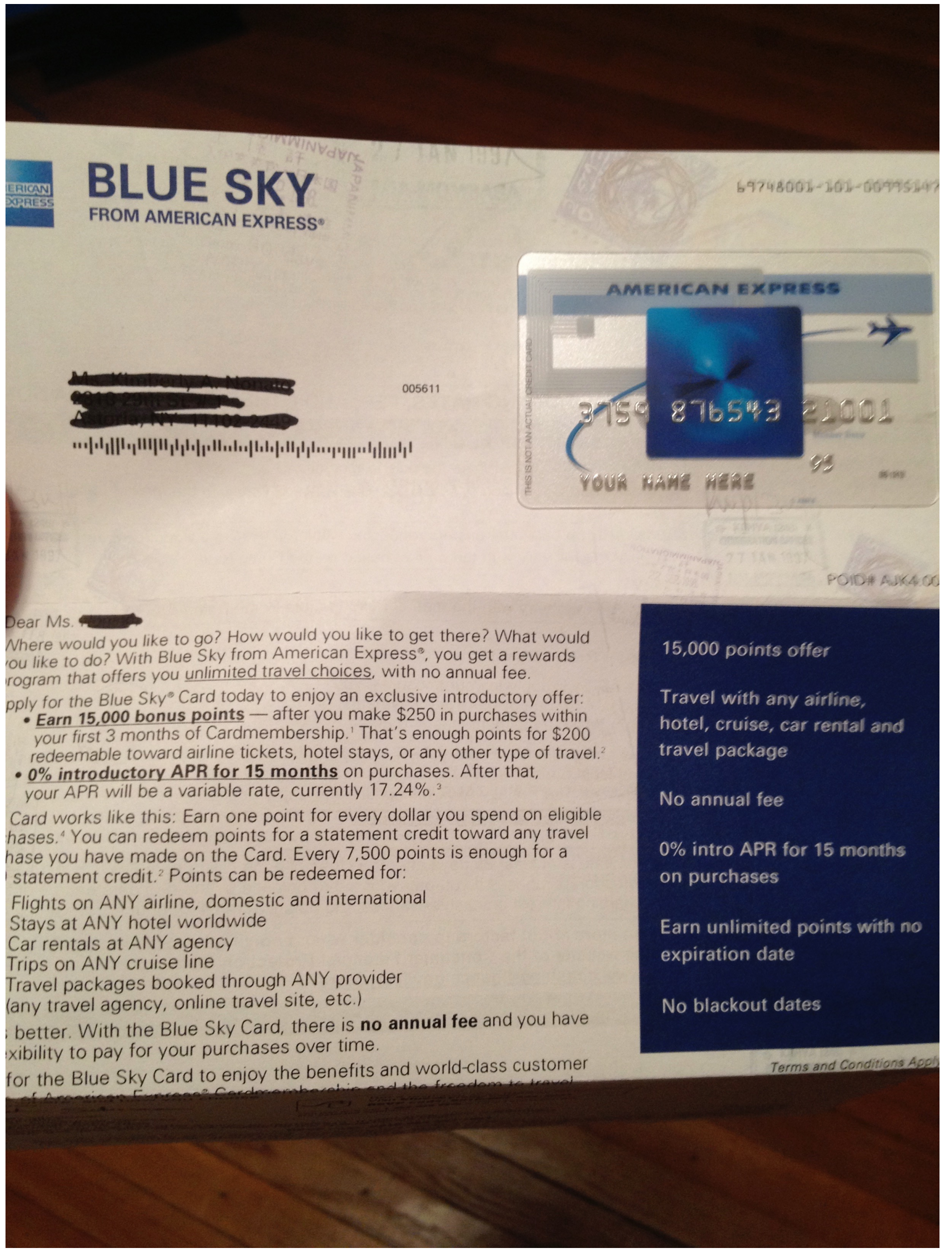
VISA
4000 1234 5678 9010
4000
GOOD THRU 12/08
B. PARKER
VISA

Skimming attack



cloning device

Another opportunity



BLUE SKY
FROM AMERICAN EXPRESS®

69748001-101-00995147

[redacted]

005611

AMERICAN EXPRESS
3759 876543 21001
YOUR NAME HERE
THIS IS NOT AN ACTUAL CREDIT CARD

POID# AJK4.00

Dear Ms. [redacted]

Where would you like to go? How would you like to get there? What would ou like to do? With Blue Sky from American Express®, you get a rewards rogram that offers you unlimited travel choices, with no annual fee.

pply for the Blue Sky® Card today to enjoy an exclusive introductory offer:

- **Earn 15,000 bonus points** — after you make $250 in purchases within your first 3 months of Cardmembership.[1] That's enough points for $200 redeemable toward airline tickets, hotel stays, or any other type of travel.[2]
- **0% introductory APR for 15 months** on purchases. After that, your APR will be a variable rate, currently 17.24%.[3]

Card works like this: Earn one point for every dollar you spend on eligible hases.[4] You can redeem points for a statement credit toward any travel hase you have made on the Card. Every 7,500 points is enough for a statement credit.[2] Points can be redeemed for:

Flights on ANY airline, domestic and international
Stays at ANY hotel worldwide
Car rentals at ANY agency
Trips on ANY cruise line
Travel packages booked through ANY provider
(any travel agency, online travel site, etc.)

better. With the Blue Sky Card, there is **no annual fee** and you have xibility to pay for your purchases over time.

for the Blue Sky Card to enjoy the benefits and world-class customer

15,000 points offer

Travel with any airline, hotel, cruise, car rental and travel package

No annual fee

0% intro APR for 15 months on purchases

Earn unlimited points with no expiration date

No blackout dates

Terms and Conditions Appl

The Johnny Carson attack

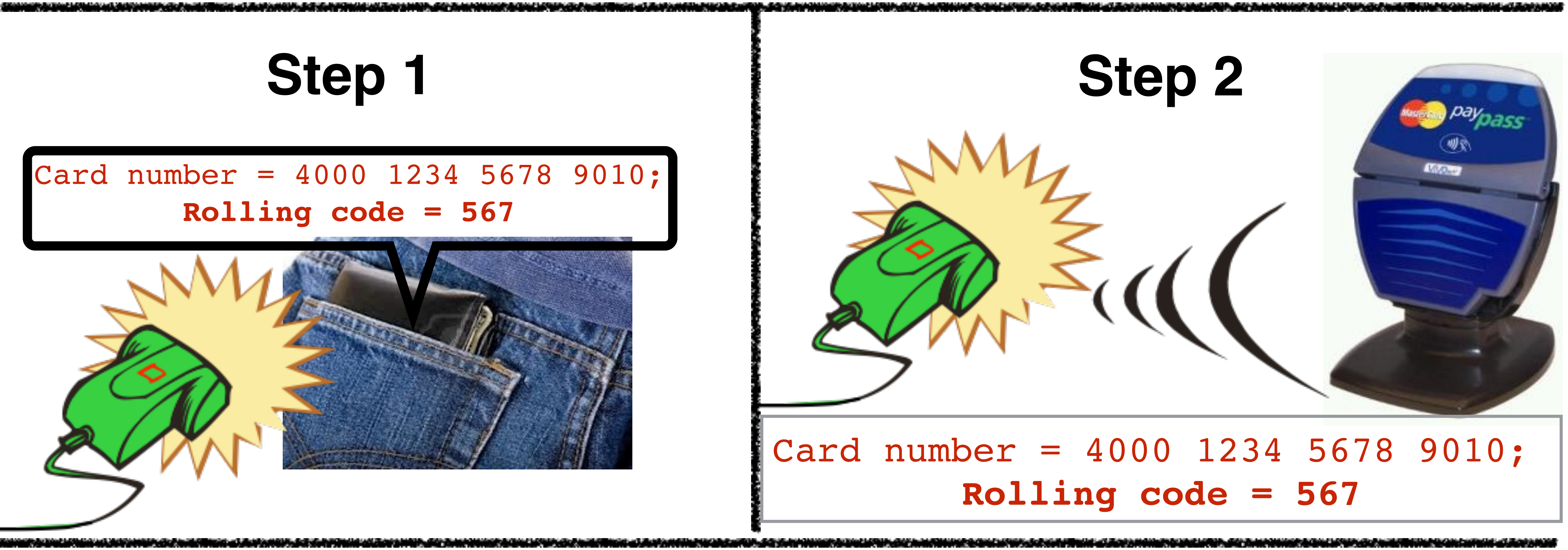
A security mechanism was therefore introduced…

Today, tap-and-go cards emit (cryptographic) validation codes (“rolling codes”).

- Transaction 1 | Code: 567
- Transaction 2 | Code: 998

S. Parker
Card number:
4000 1234 5678 9010
Exp: 12/08
Rolling code: 567

But skimming still possible!



Step 1

Card number = 4000 1234 5678 9010;
Rolling code = 567

Step 2

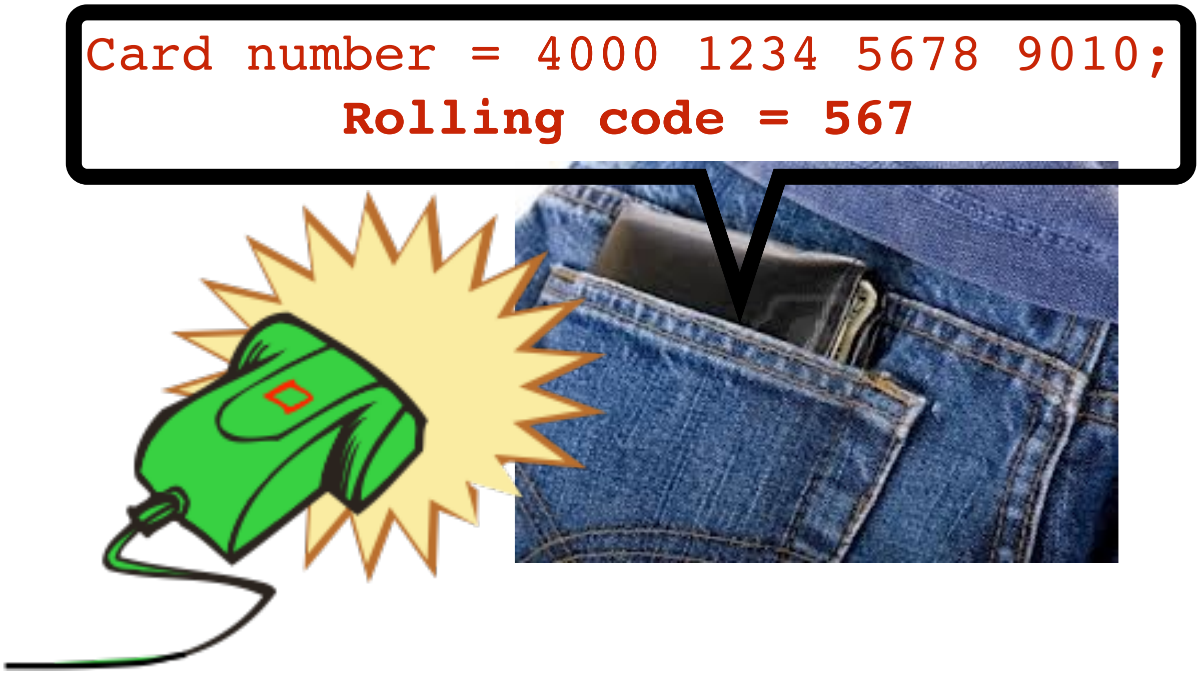
Card number = 4000 1234 5678 9010;
Rolling code = 567

The adversarial game

- Adversary enters a “race condition” with the consumer.
- If consumer spends first, adversary’s code is invalidated.
- If the adversary spends first, she wins.

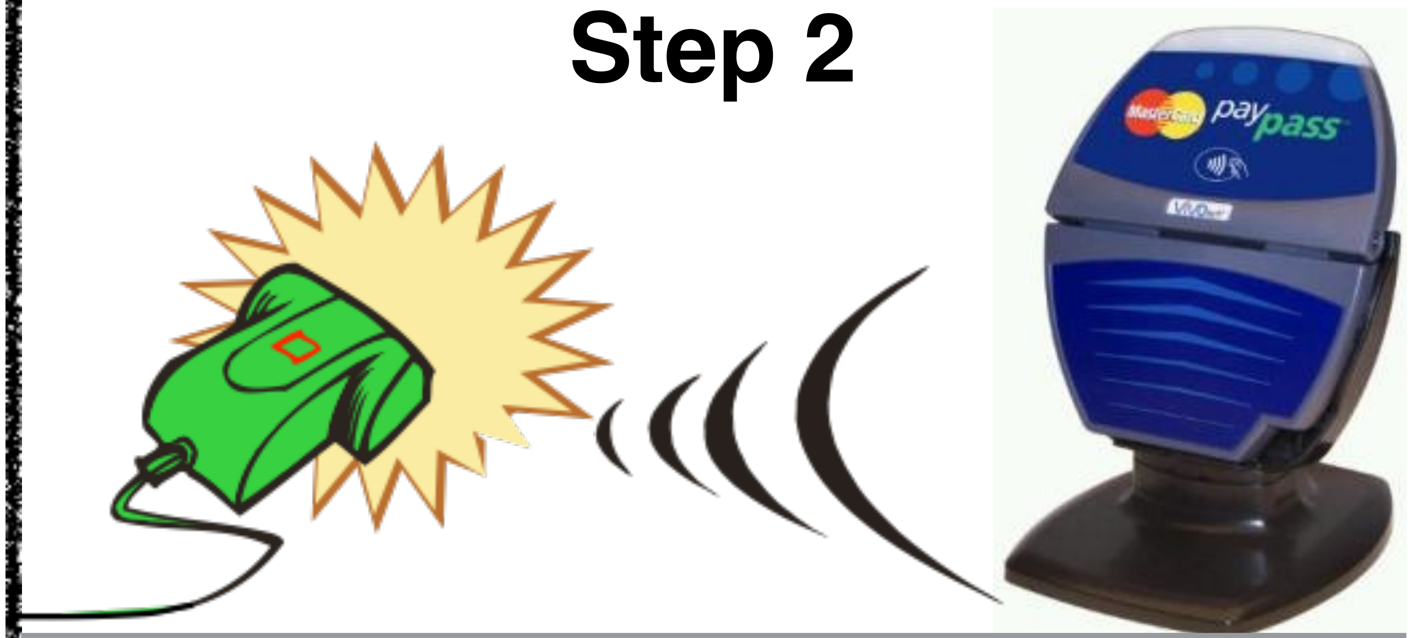
~~Transaction 1 | Code: 567~~
Transaction 2 | Code: 998

Step 1



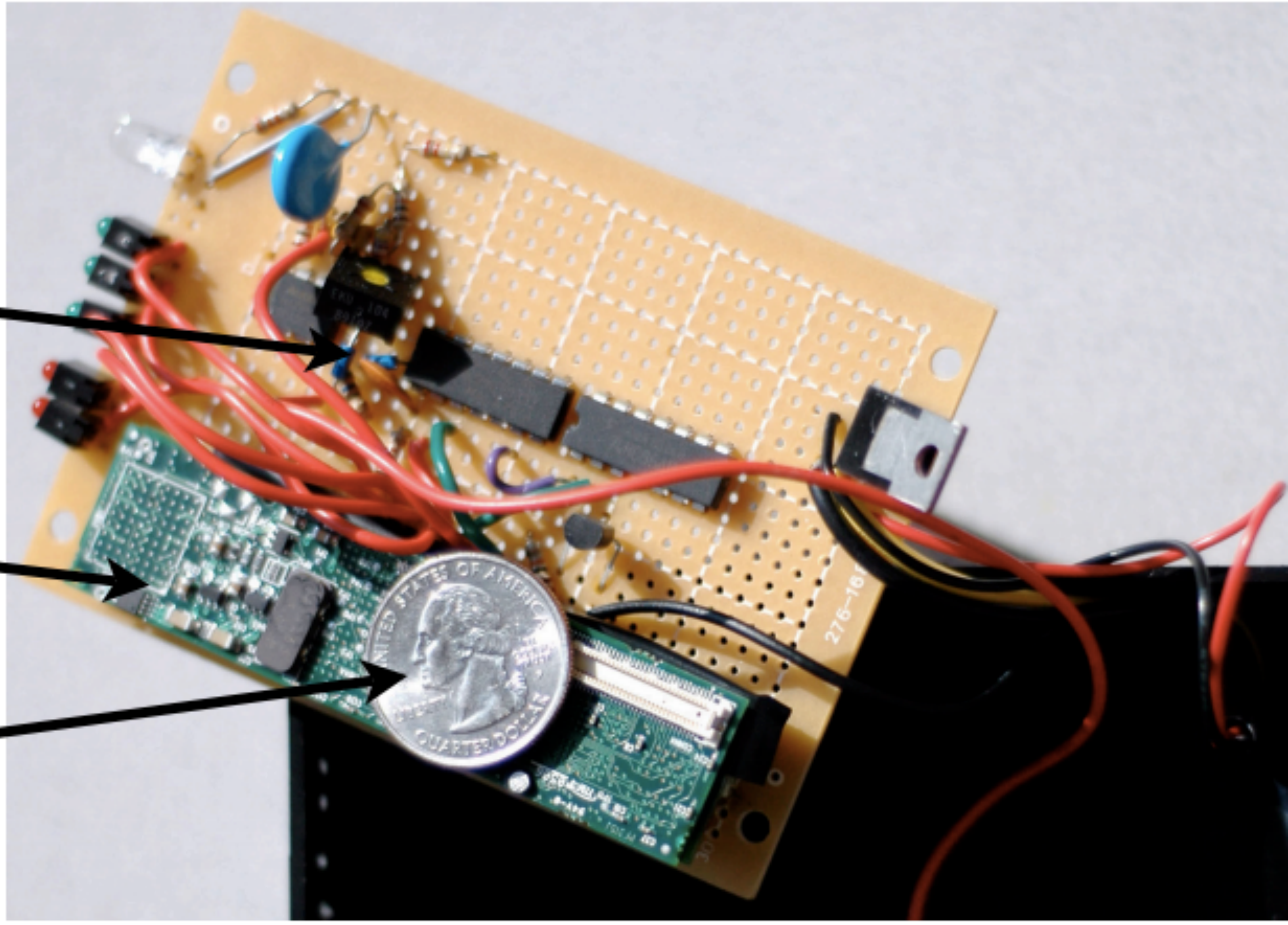
```
Card number = 4000 1234 5678 9010;
      Rolling code = 567
```

Step 2



```
Card number = 4000 1234 5678 9010;
      Rolling code = 567
```

Cloning device from 2007 study

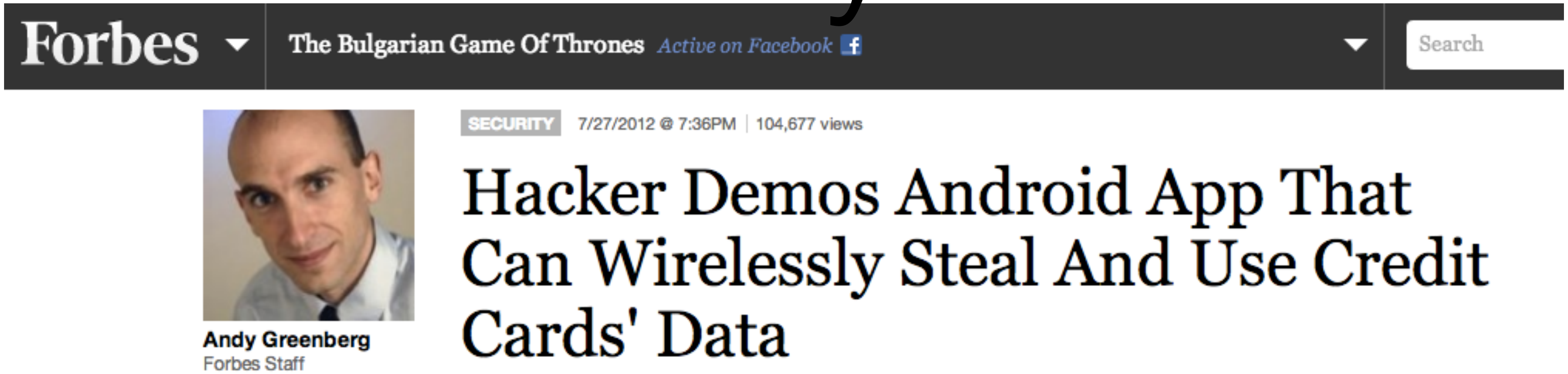


"CS style" modulation

Gumstix w/ Linux

George Washington

Today



Forbes

The Bulgarian Game Of Thrones *Active on Facebook*

Search

SECURITY 7/27/2012 @ 7:36PM | 104,677 views

Hacker Demos Android App That Can Wirelessly Steal And Use Credit Cards' Data

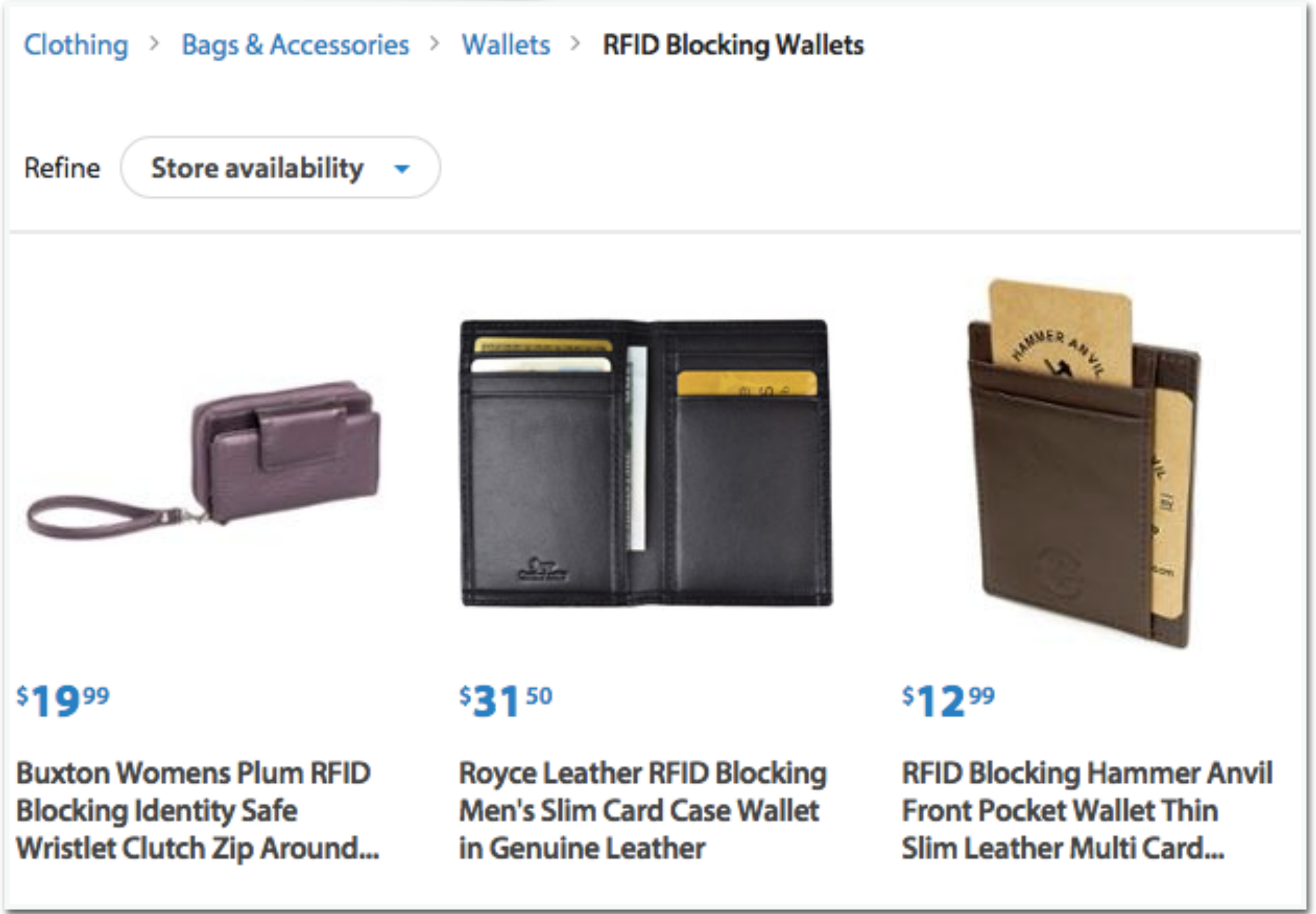
Andy Greenberg
Forbes Staff

Eddie Lee's Android phone, displaying data it has wirelessly

Google Wallet and Apple Pay

Card skimming defenses

Walmart



Clothing > Bags & Accessories > Wallets > RFID Blocking Wallets

Refine Store availability

$19 99	$31 50	$12 99
Buxton Womens Plum RFID Blocking Identity Safe Wristlet Clutch Zip Around...	Royce Leather RFID Blocking Men's Slim Card Case Wallet in Genuine Leather	RFID Blocking Hammer Anvil Front Pocket Wallet Thin Slim Leather Multi Card...

Referenced June 2015

The Fox News approach

How likely are attacks on tap-and-go cards in practice?

- Question of **incentives**
- Is this really the best way to steal credit-card information?
- Is it the best way to track users' physical movements?

What about mobile devices?

- How serious is the tap-and-go risk in
    - iPay
    - Android Wallet

Anatomy of a wallet

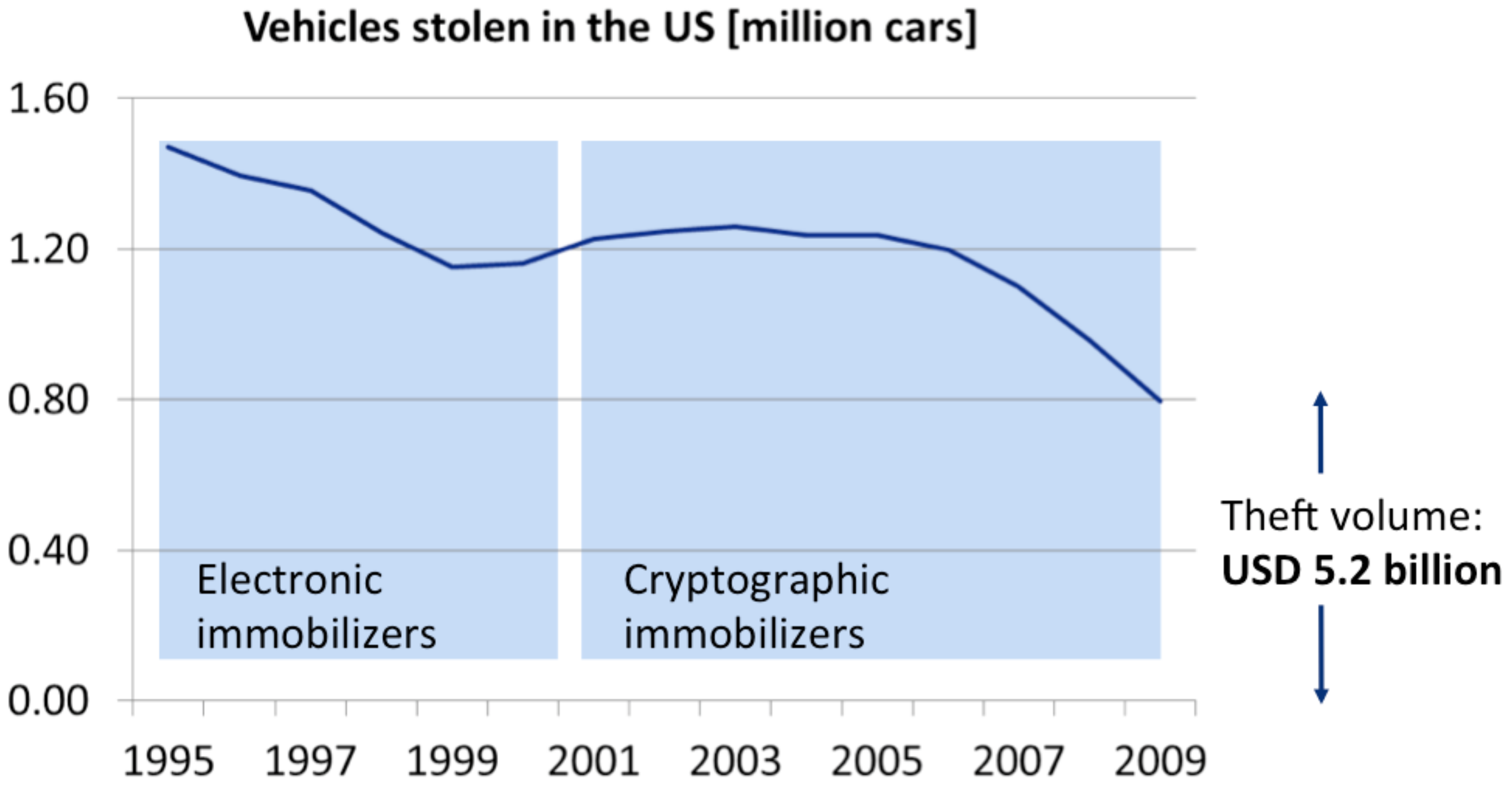
ROVER
SOCIAL SECURITY
123-45-6789
THIS NUMBER HAS BEEN ESTABLISHED FOR
JOHN Q PUBLIC
SIGNATURE
FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
ID 228 60 B
TWENTY DOLLARS
HID
MasterCard
5412 7512 3412 3456
12-09
S. MORRIS
VISA
4000 1234 5678 9010
12/08
B. PARKER
LIBERTY
IN GOD WE TRUST
2013
UNITED STATES OF AMERICA
QUARTER DOLLAR
2012

Automobile ignition keys

- Also contain RFID tags
- They perform cryptographic authentication protocols with automobile "immobilizer."
- Without right chip, car won't start.

Image credit: Karsten Nohl

Apparently quite successful in reducing rate of theft



Source: FBI Uniform Crime Report (2009)

Image credit: Karsten Nohl

Various vulnerabilities

	Key length	Cipher strength	Protocol strength
DST 40	🙁	😐	🙂
DST 80	🙂	😐	🙂
Hitag 2	🙁	🙁	🙂
Hitag 3	🙂	🙁	🙂
Hitag AES	🙂	🙂	🙂
Megamos	🙂	😐	🙁

Image credit: Karsten Nohl

“Stealing” car

“Stealing” gas

TI DST cracking

(The problem with 40-bit keys)

Stubblefield, Rubin, Bono, and Green (JHU, 2004)

Why did they use weak keys?

Anatomy of a wallet

Isn’t cash almost obsolete?

- You probably don’t have one of these in your wallet.
- Yet there was $863.1 billion in $100 bills (or 8.631 billion notes) in circulation as of the end of 2012.
  - That’s $2800+ for *every inhabitant of the U.S.*
- 75%+ of value of U.S. currency is denominated in $100 bills!
- How many of us own twenty-eight $100 bills?
- **Where is all of it?**

100
ONE HUNDRED DOLLARS
THE UNITED STATES OF AMERICA
FEDERAL RESERVE NOTE
JB 00000000 T
B2
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
SPECIMEN
Secretary of the Treasury.
Treasurer of the United States.
FRANKLIN
SERIES 2009
JB 00000000 T
100

Most U.S. currency is probably not in the U.S. (60%+)

Figure 6B: Simple Estimates of the Value of U.S. Currency Abroad

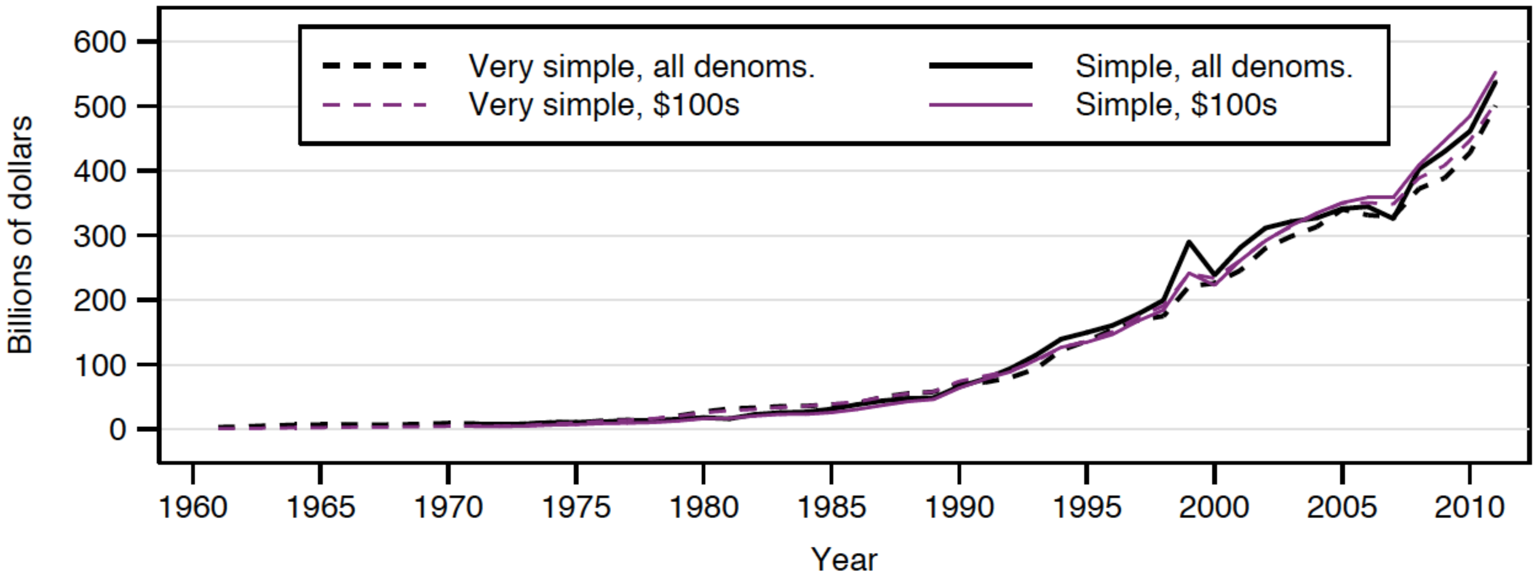
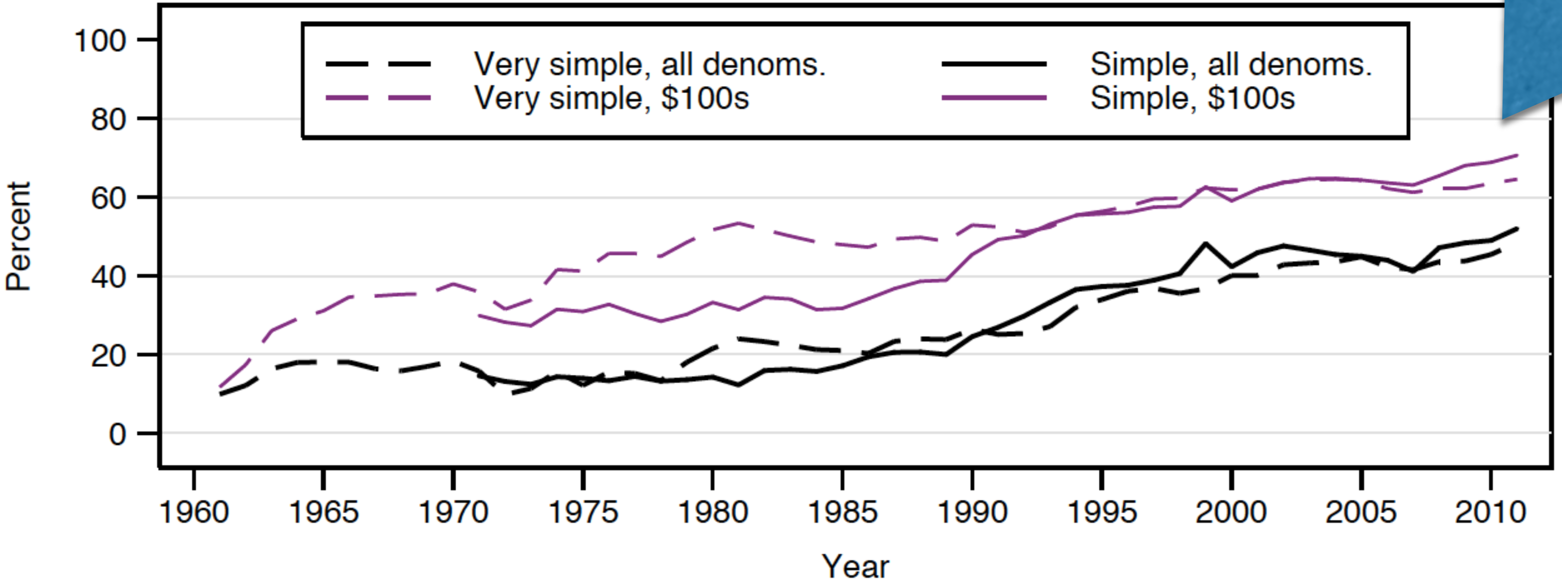


Figure 6A: Simple Estimates of the Share of U.S. Currency Abroad



Source: R. Judson. Crisis and Calm: Demand for U.S. Currency at Home and Abroad from the Fall of the Berlin Wall to 2011. Board of Governors of the Federal Reserve System. International Finance Discussion Papers. IFDP 1058. November 2012.

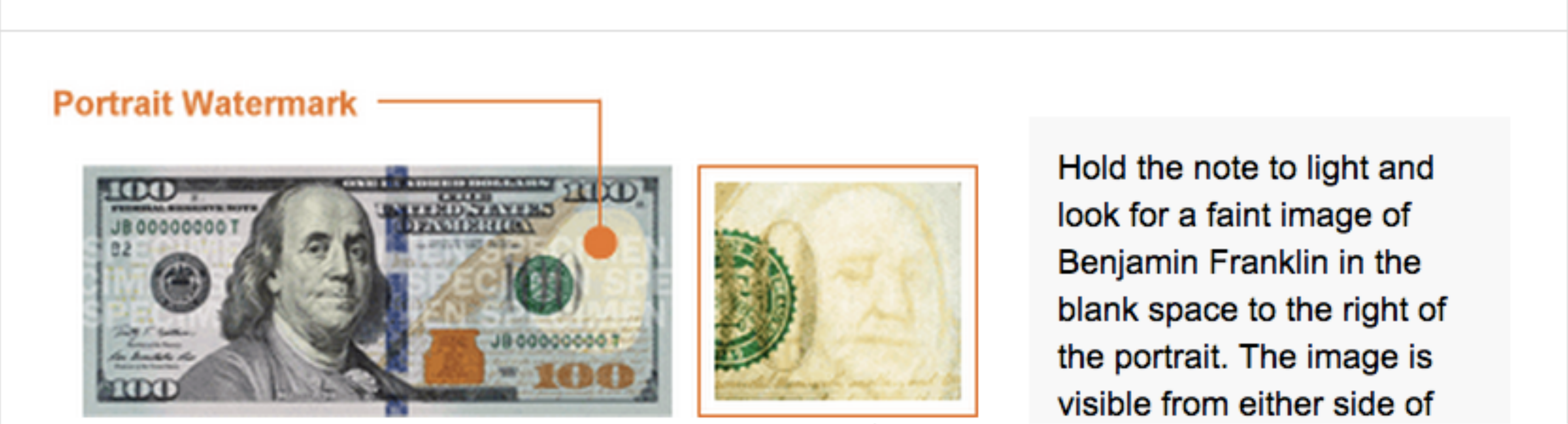
What does this have to do with security?

- Remember that **incentives** are a key question.
- Most U.S. currency is denominated in $100 notes.
- Demand is rapidly growing.
- Many or most transactions involving these notes are outside U.S. jurisdiction (and range of direct U.S. law enforcement).
- So forgery of $100 bill must be extremely lucrative…
- …and thus a severe problem!

2013 $100 bill redesign

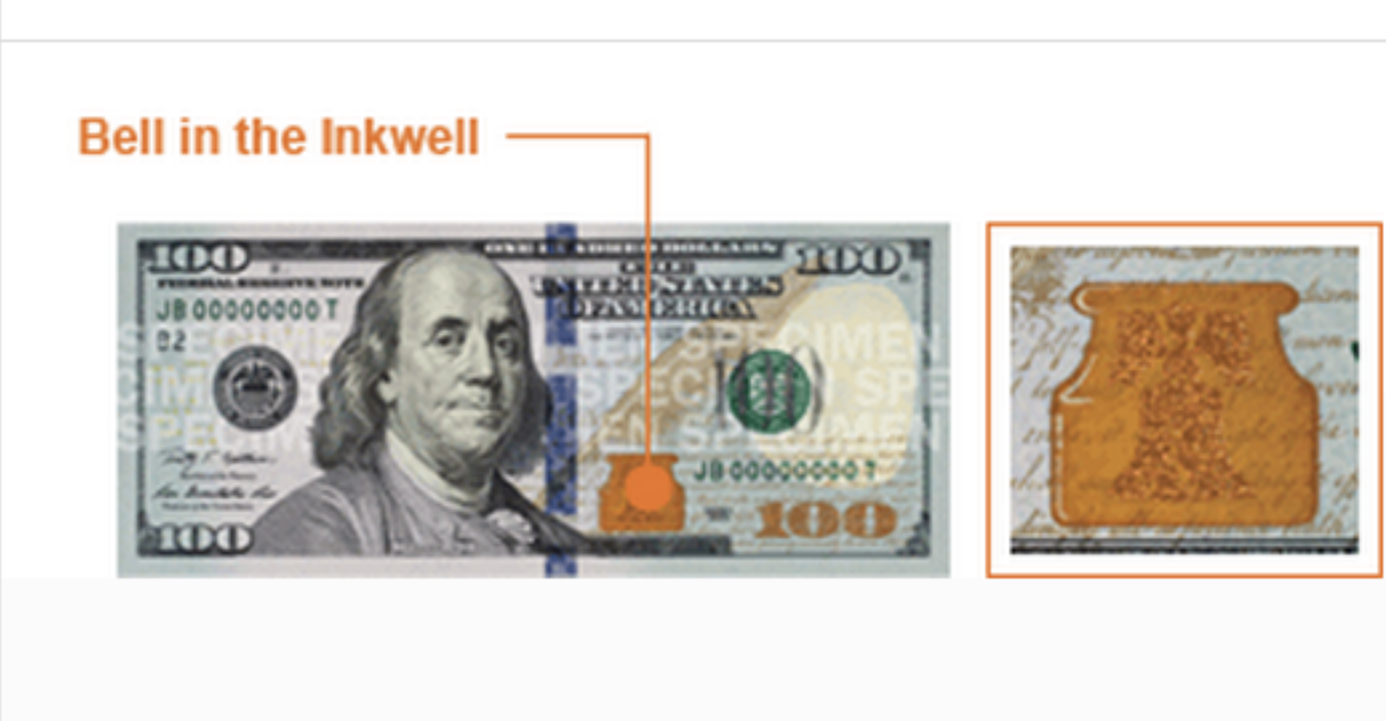
- 10 years of research into anti-counterfeiting features
- 12.7¢ per bill production cost vs. 7.8¢ for previous version
- More security features than any other U.S. banknote

- More

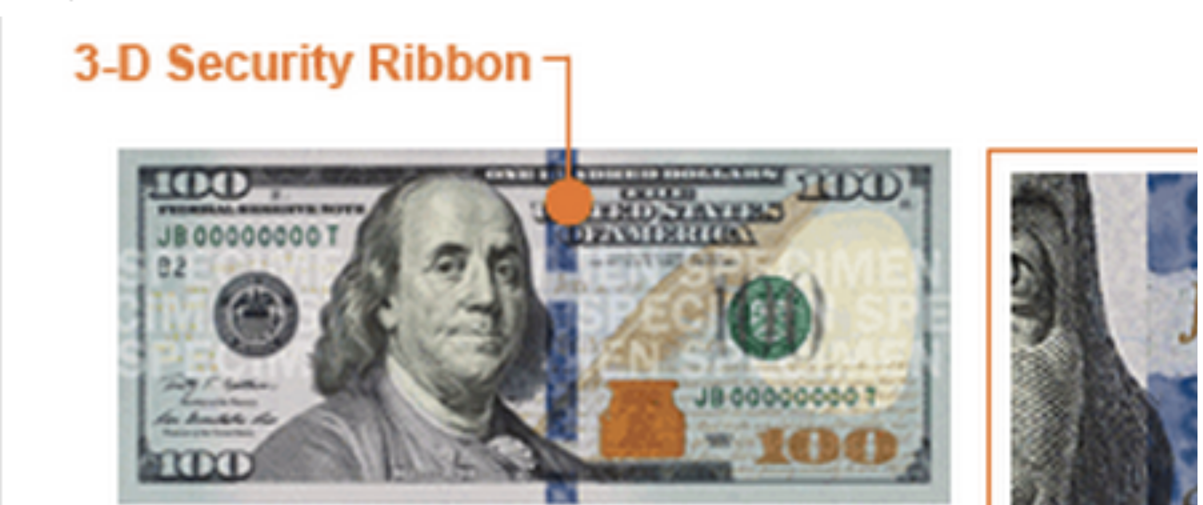


Portrait Watermark

Hold the note to light and look for a faint image of Benjamin Franklin in the blank space to the right of the portrait. The image is visible from either side of

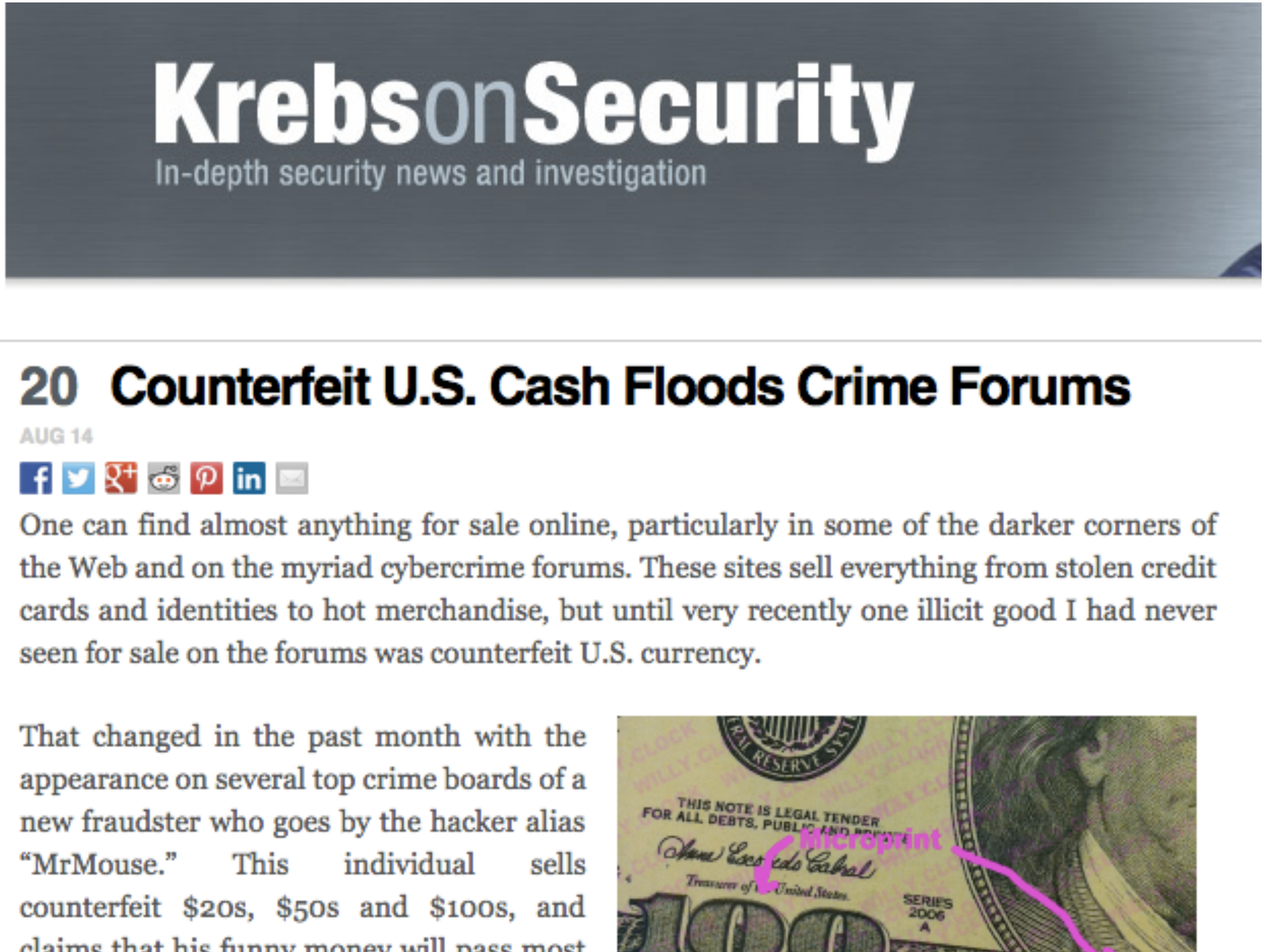


Bell in the Inkwell



3-D Security Ribbon

Disney dollars



KrebsonSecurity

In-depth security news and investigation

20 AUG 14 Counterfeit U.S. Cash Floods Crime Forums

One can find almost anything for sale online, particularly in some of the darker corners of the Web and on the myriad cybercrime forums. These sites sell everything from stolen credit cards and identities to hot merchandise, but until very recently one illicit good I had never seen for sale on the forums was counterfeit U.S. currency.

That changed in the past month with the appearance on several top crime boards of a new fraudster who goes by the hacker alias "MrMouse." This individual sells counterfeit $20s, $50s and $100s, and claims that his funny money will pass most

Why not print $500 bills?

- “U.S. currency is a preferred medium of exchange for facilitating clandestine transactions, and for storing illicit and untaxed wealth…These include the illegal trade in drugs, arms and human trafficking as well as the amount of “unreported” income, that is, income not properly reported to the fiscal authorities due to noncompliance with the tax code.”
- The Euro zone prints a 500 Euro (approx $675) banknote.
- The U.K. no longer sells them in money exchange offices.
- In 2010: Serious Organised Crime Agency: “90% of all €500 notes sold in the UK are in the hands of organised crime.”

Great lesson in **incentives**

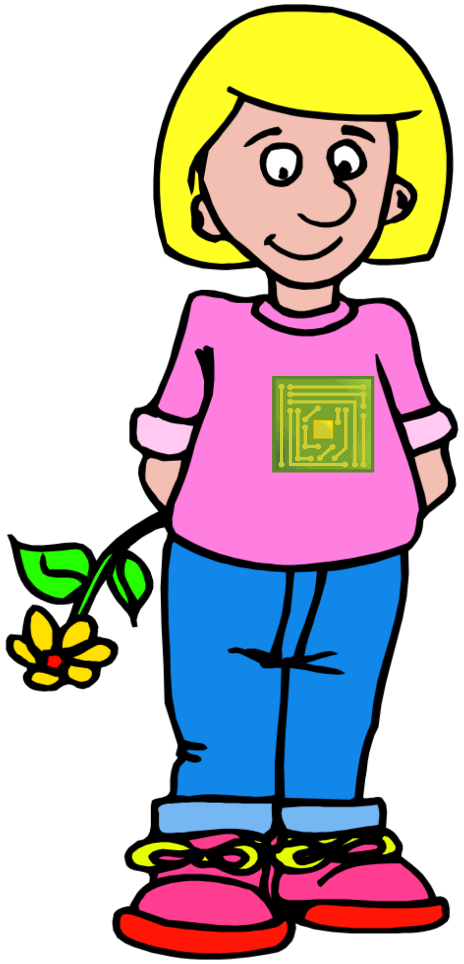
- “Follow the money” is an important way to understand incentives.
- True in many areas of cybersecurity
- For example, UCSD study of illegal online prescription market (spam for Viagra, forum abuse, etc.)
    - McCoy et al. PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. 2012.
- Money flows through a few major affiliate programs and a few banks processing transactions.
- Huge amount of spam potentially eliminated by shutting down these programs and banks

Anatomy of a wallet

HID proximity card

- Some varieties even more vulnerable than tap-and-go credit-card
    - Basically a wireless barcode
- Cloning attack by Jonathan Westhues in 2006
    - http://cq.cx/prox.pl
- Any better today? Good class project…

Human location tracking



CORNELL TECH

RFID and other wireless proposed for

- Schools
- Amusement parks
- Hospitals

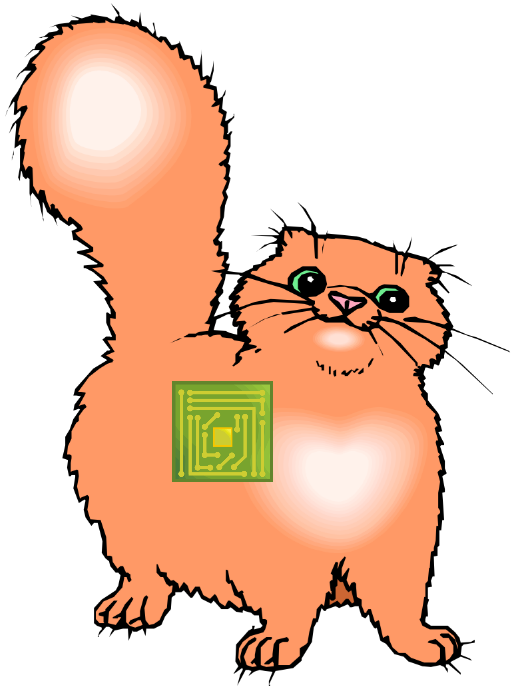
mynd

We Keep Kids From Getting Lost

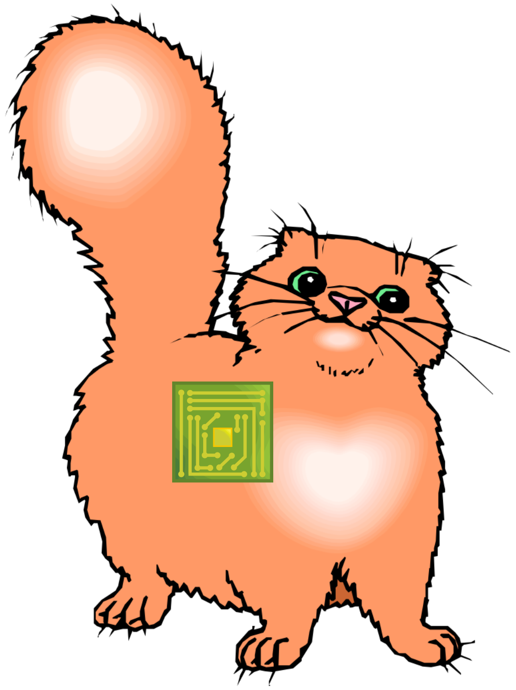
RFID also used to track…

50+ million housepets in U.S. are "chipped"

A riddle…

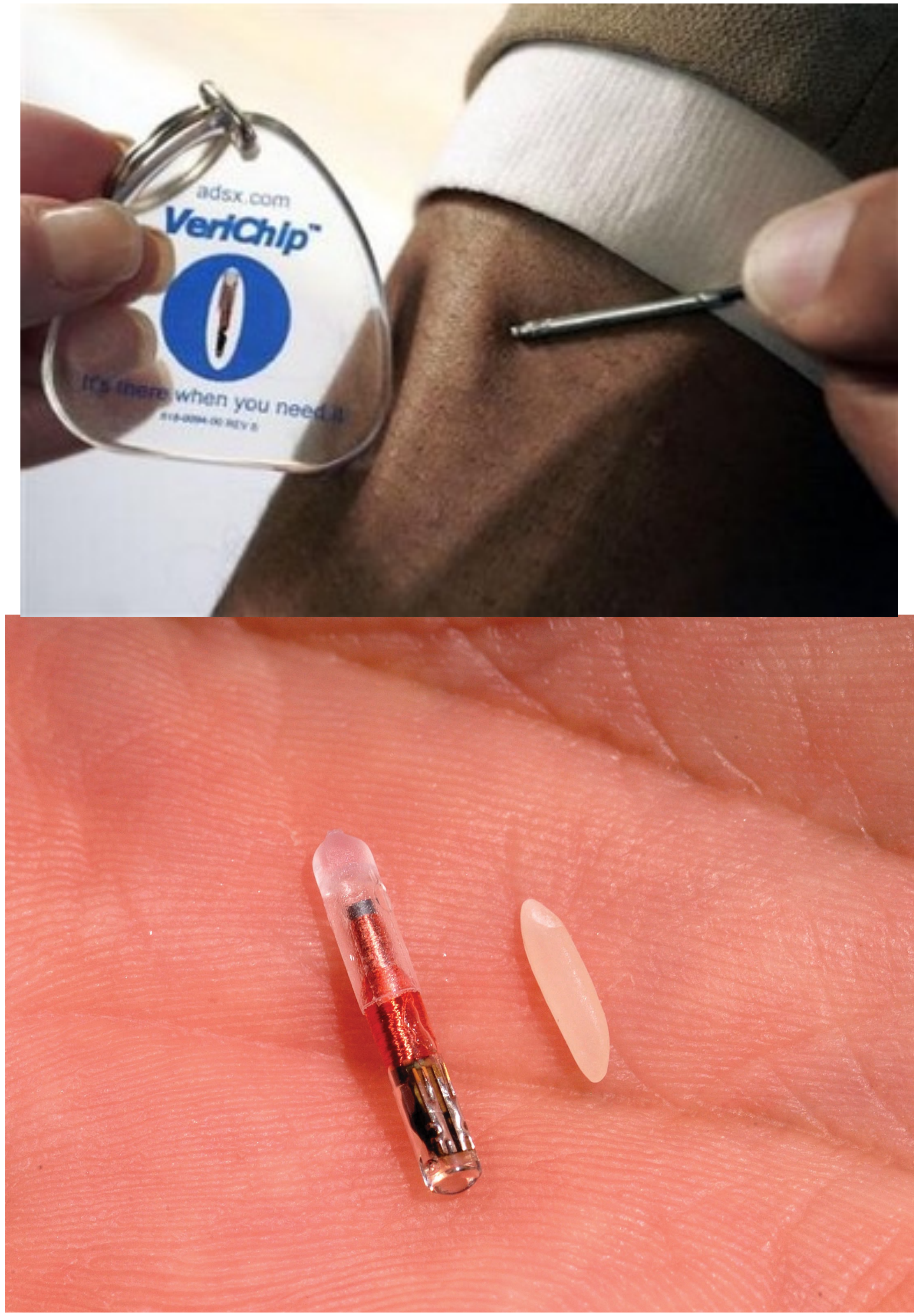
 + = ???

Human-implantable RFID



+

=



VeriChip^{TM}

www.rapturechrist.com/666.htm

MARK TECH: 666

- NEW Subdermal Biochip Implant for Cashless Transactions - is it the Mark?

The **mark** is a microchip assembly which will be implanted under the skin of the right hand. **Later on, the mark will be implanted under the forehead, so people who have no right hand could also have the mark.** The microchip assembly, called radio frequency identification (RFID) is already used in animals.
In dogs, the RFID is placed between the shoulder blades, and in birds it is implanted under the wing.
Now there is a one for humans called **VeriChip™**.

OBAMACARE
HEALTH PLANS
Click to Enroll
Call Now: 1-800-508-6754

Ads by +HealthNetwork

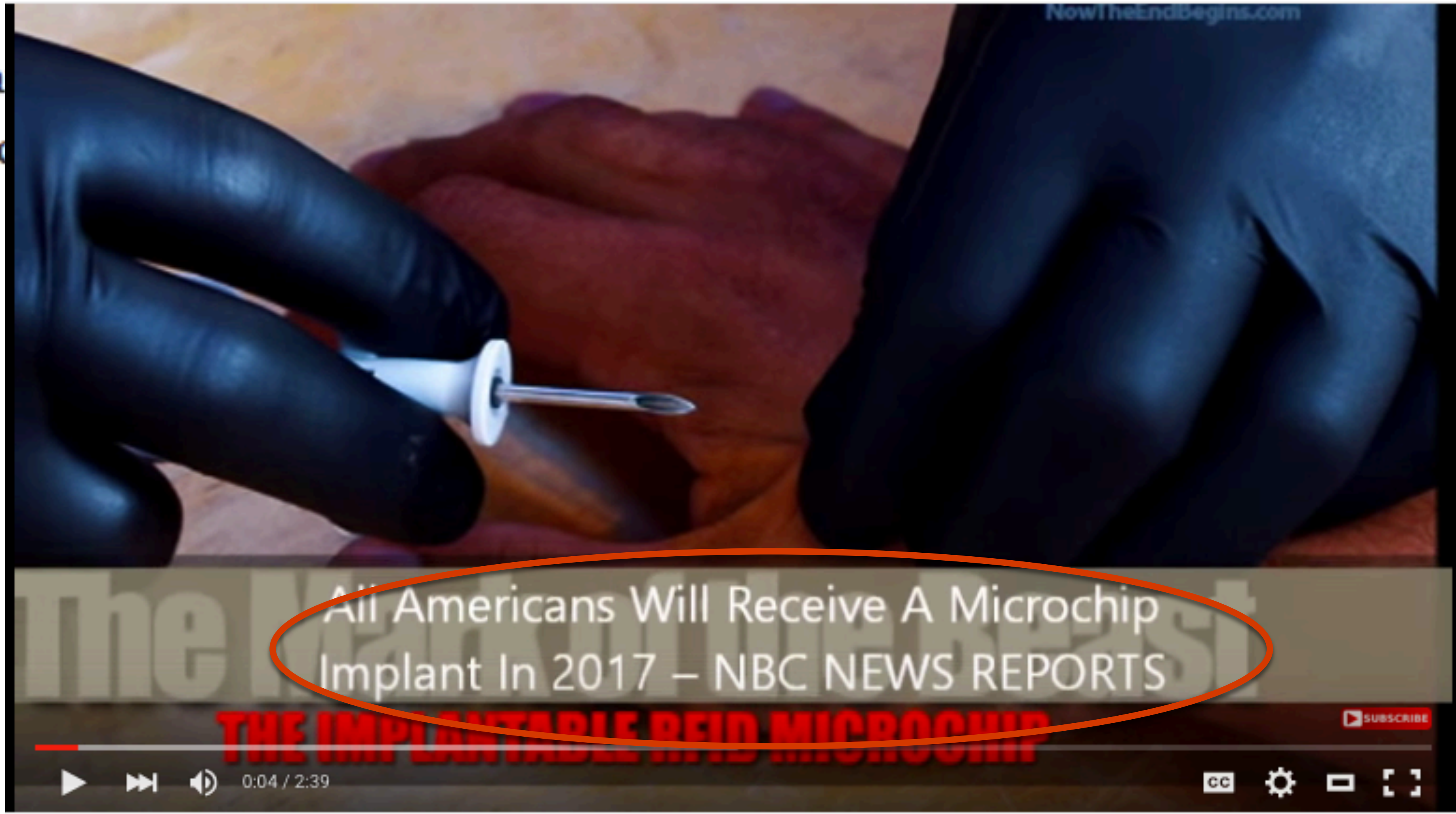
Compare Health Insurance

Affordable Care Act Plans

Obamacare Health Plans

What is the Truth Behind the ObamaCare Microchip Implant Rumor?

We look at the truth behind the Oba
Care Act contains mandatory microc

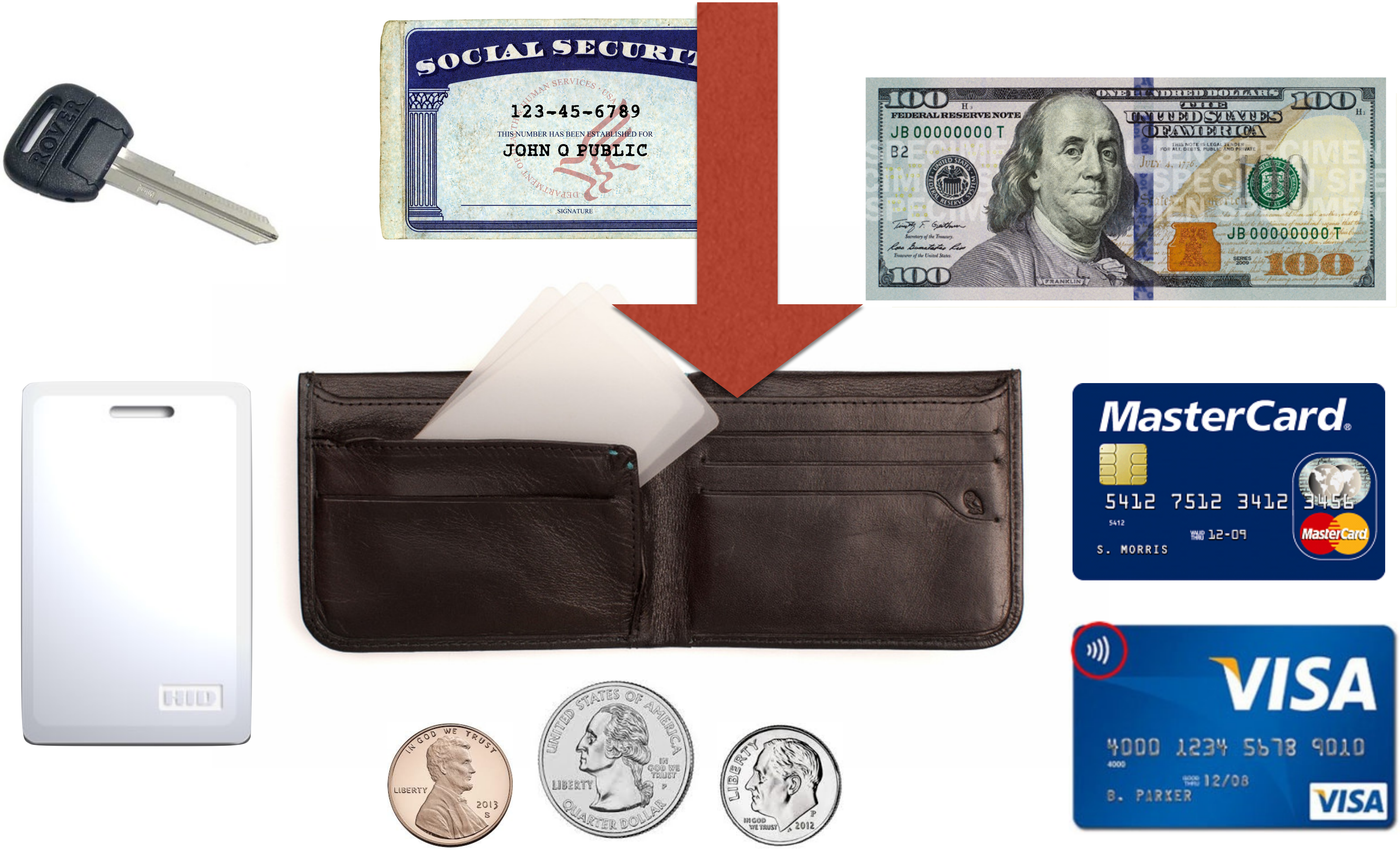


All Americans Will Receive A Microchip Implant In 2017 – NBC NEWS REPORTS

Human-implantable RFID

- Proposed for medical-patient identification
- *Also* proposed and used as an authenticator for physical access control, a “prosthetic biometric”
- E.g., Mexican attorney general purportedly used for access to secure facility
- What kind of cryptography does it have?
  - None: It can be easily cloned
  - [Halamka et al. ‘06]
- So shouldn’t we add a challenge-response protocol?
- Cloning may actually be a *good* thing

Anatomy of a wallet



The hidden compartment

- Used to conceal bulk of cash
- Security through obscurity…

The hidden compartment

- Works in part because most wallets don’t have one
- If *everyone* had one, what would happen?
- Security is not just an arms race, it’s a race from a bear…

“I don’t need to outrun a bear. Only you.”

Not just an arms race…

- In system design, this means in practice that it’s most helpful to be more secure than others.
- Why? Incentives. (Economics.)

The shape of the wallet is changing

Which security goals, adversarial models, mechanisms, and incentives will remain the same? Which will change?

Lecture takeaways

- Your wallet is interesting, and chock full of security technologies, e.g.,
  - Cryptographically enabled chips
  - Tamper evident hardware (coins and smartcards)
  - Anti-forgery devices
- Vulnerabilities often arise when new technologies get introduced with old adversarial models
  - E.g., tap-and-go credit cards
- "Follow the money" is a great way to understand incentives
  - E.g., $100
- Security is often about outrunning others, not the bear…