Your Wallet

Thanks to Ari Juels for this deck!
“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 previous classes, 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…

fourées

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).
Here’s the same trick in phishing e-mail
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…
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 3 (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

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."

- Instant validity check; refund for invalid cards

- Payment in Bitcoin
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...

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
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).
- Finally came to U.S in 2015
- Merchants in U.S. 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. now that we have them?
  - 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
Skimming attack
Another opportunity
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.
Cloning device from 2007 study

“CS style” modulation

Gumstix w/ Linux

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

Google Wallet and Apple Pay
Card skimming defenses

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?
Anatomy of a wallet
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

Various vulnerabilities

<table>
<thead>
<tr>
<th>Key length</th>
<th>Cipher strength</th>
<th>Protocol strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>DST 40</td>
<td>😞</td>
<td>😊</td>
</tr>
<tr>
<td>DST 80</td>
<td>😊</td>
<td>😊</td>
</tr>
<tr>
<td>Hitag 2</td>
<td>😞</td>
<td>😊</td>
</tr>
<tr>
<td>Hitag 3</td>
<td>😊</td>
<td>😊</td>
</tr>
<tr>
<td>Hitag AES</td>
<td>😊</td>
<td>😊</td>
</tr>
<tr>
<td>Megamos</td>
<td>😊</td>
<td>😞</td>
</tr>
</tbody>
</table>

Image credit: Karsten Nohl

“Stealing” car

“Stealing” gas
TI DST cracking
(The problem with 40-bit keys)

Stubblefield, Rubin, Bono, and Green (JHU, 2004)
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?
Most U.S. currency is probably not in the U.S. (60%+)
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
Disney dollars

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 of the tests that merchants use to tell bogus bills from the real thing.

MrMouse markets his fake funds as “Disney Dollars,” and in addition to blanketing some of the top crime forums with Flash-based ads for his service he has boldly paid for a Reddit stickied post in the official Disney Market Place.
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 printed a 500 Euro (approx $675) banknote until 2019

• 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.)

• 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](http://cq.cx/prox.pl)
- Any better today? Good class project…
Human location tracking

RFID and other wireless proposed for
- Schools
- Amusement parks
- Hospitals
RFID also used to track…

50+ million housepets in U.S. are "chipped"
A riddle…

+ = ???
Human-implantable RFID
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™.**
Ripped from the headlines

Wisconsin Company Offers To Implant Chips In Its Employees

July 25, 2017 - 2:06 PM ET
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?
Anatomy of a wallet
The hidden compartment

- Used to conceal bulk of cash
- 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?
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…