# Lecture 1

### CS-466 Applied Cryptography Adam O'Neill

# Crypto Games!!!

# **Class Logistics**

3





Instructor: Adam O'Neill; adamo@cs.umass.edu Office Hours: Tues & Thurs before class (roughly 2:45-3:45pm) or by appointment, LGRC 329A (Low-rise)

Course website: https://people.cs.umass.edu/~adamo/sp19466/index.html

TA: Albert Williams; abwillia@cs.umass.edu Office Hours: Weds 2-3pm, LGRT 220 (High-rise)



### Grades: 50% problem sets, 25% midterm, 25% final

Final grades are are given according to equivalence classes via a formula which depends on the scores. **If you all do well you all get an A.** 

For problem sets, you can discuss or use any resource but must list your collaborators/resources. Write your final solutions by yourself. Please typeset them. Turn in PDF via procedure detailed later.

# Some Additional Resources

Bellare's courses http://cseweb.ucsd.edu/~mihir/cse107/ http://cseweb.ucsd.edu/~mihir/cse207/

#### **Rogaway's Courses**

http://web.cs.ucdavis.edu/~rogaway/classes/ 127/winter19/

#### **Boneh's Courses**

http://crypto.stanford.edu/~dabo/courses/cs2 55\_winter18/

Boneh-Shoup Book https://crypto.stanford.edu/~dabo/cryptobook

Katz-Lindell book http://www.cs.umd.edu/~jkatz/imc.html

Reyzin Course

https://www.cs.bu.edu/~reyzin/teaching/f14c s538/

# How to do well in this course

- Don't focus on your grade, just try your best
- Be adventurous, quizzical
- Think of the class as telling a story
- Try to make your thoughts rigorous and precise, in the language of mathematics

http://cseweb.ucsd.edu/~mihir/education.html

# What's cryptography?

3

# What's Cryptography?

## One viewpoint (Goldreich):

How to communicate and compute in the presence of an adversary.

Cryptography is a part of science in the same way as math or physics.





# What's Cryptography?

## Another viewpoint (Bellare/Rogaway):

There is no such thing as **Cryptography**, really.



How many can you name?

# What's Cryptography?

Another viewpoint (Bellare/Rogaway):

Cryptography is socially constructed.

Cryptography is alive, not a textbook!

See <a href="http://web.cs.ucdavis.edu/~rogaway/papers/cc.pdf">http://web.cs.ucdavis.edu/~rogaway/papers/cc.pdf</a>

# The analogy to art





There is no such thing as "secure encryption scheme" ontologically But still we need a definitions that are

- Precise
- Useful

# Security Mindset

Put on your adversary hat!

Ask what the risks and threats are. How might the system be attacked?

Be critical of security claims.

Our system is secure because it uses 128-bit keys! How are they being used? What is the threat model? Do you have a security proof?

### Coloring outside the lines



"Hey! They're lighting their arrows! Can they do that?"

🛛 Marc Sniukas - Doujak Corporate Developmen

# Some goals and uses

3

# Who Uses Crypto?



You probably did, today!

- TLS/SSL protocol (used for Gmail, Facebook, YouTube...)
- 10000+ apps use crypto... most incorrectly ⊗

https://www.cs.ucsb.edu/~chris/research/doc/ccs13 cryptolint.pdf

## SSL/TLS



*K* is a fresh, authentic session key Adversary cannot influence or know *K* 

## SSL/TLS

### **TLS/SSL Vulnerabilities**

Vulnerability	crypto	Implementation/ Usage
FREAK	х	
<b>Re-negotiation</b>	х	
Version Rollback		x
BEAST	х	
Padding Oracle	х	
Lucky 13	х	
Poodle	х	x
Heartbleed		x
RC4	х	
AllYourSSLsAreBelongToUs		x

Many different TLS/SSL Implementations: OpenSSL, GnuTLS, cryptlib, JSSE, RSA BSafe, SChannel, ...

Issues: Cipher suites, re-negotiation, sidechannels, buffer overflows, bad randomness, ...

Lots of bad crypto in TLS/SSL, often for historic and legacy reasons.

## Secure Channels: Ideal

## Secure Channels: Real

# Security goals

# The question of identity



On the Internet, nobody knows you are a dog.

# **Example applications**

# Crypto beyond secure channels

# Why does it matter?

3

# Adversaries are real!

Academic cryptographers often represent the adversary like this





Instead think of the adversary as a well-funded, technically capable and highly motivated entity with lots of computing power.

### Does it matter to you?

If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.

#### Glenn Greenwald



If you have nothing to hide then give me the passwords to ALL your email accounts, your text and chat histories, ...

https://www.youtube.com/watch?v=pcSlowAhvUk 20 minute video of TED talk

> The Chronicle of Higher Education Why privacy matters even if you have nothing to hide http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

Bruce Schneier The Value of Privacy Privacy protects us from abuses by those in power ... We keep private journals, sing in the shower ... privacy is a basic human need. https://www.schneier.com/blog/archives/2006/05/the\_value\_of\_pr.html

http://zeroknowledgeprivacy.org/library/why-privacy-matters/



Eric Schmidt, CEO Google, 2009

# Snowden revelations



theguardian

News World news ) The NSA files

eries: Glann Greenwald on security and Eberty

Read the Verizon court order in full here Obama administration justifies surveillance lens Greenwald he Guardian, Wednesday 5 June 2013 mo to corromento / ws ) World news ) NSA eries: Glenn Greenwald on security and liberty NSA collected US email records in bulk an two years under Obama Court-approved NSA access to Google and Yahoo accounts runched by Bush continued 'until 2011' The III d collection order every 90 days Verizon hands phone records of millions of customers to NSA daily rams still mine US internet metadata Extensive wiretapping, tapping undersea cables pencer Ackerman 27 June 2013 11 20 ED1 Harvesting of millions of email and instant-messaging contact lists Tracking and mapping location of cellphones Backdoor planted in Dual EC DBRG random-number generator Paying corporations to adopt NSA-broken standards V York at Sophisticated malware

News World news US national security Series: Gienn Greenwald on security and liberty

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over

all call data shows scale of domestic surveillance under Obarna

resource reasons. Photograph Patio Marthez Monsenze/PP The Obama administration for more than two years permitted the National Sociumy Agency to continue collecting vast amounts of records details in the email and intermet usage of Americans, according to secret

The documents indicate that under the program, launched in 2001, a federal judge sitting on the secret surveillance panel called the Fisa

court would approve a bulk collection order for internet metadata "every

90 days". A senior administration official confirmed the program, stating

documents obtained by the Guardian.

that it ended in 2011

News World news ) The NSA files

New NSA leaks show how US is bugging its European allies Exclusive: Edward Snowden papers reveal 38 targets including EU, France and Italy

Berlin accuses Washington of cold war tactics

#### 📑 Follow Julian Borger by email 🌆

Even MacAskill in Rio de Janeiro and Julian Borger The Guardian, Sunday 30 June 2013 16:28 EDT Jump to comments (2843)

#### News World news NSA

Series. Glenn Greenwald on security and liberh

Microsoft handed the NSA access to encrypted messages • Secret files show scale of Sikton Valley co-operation on Prism • Outlook core encryption wirelede even before official launch

Skype worked to enable Prism collection of video cats
Company says it is legally competied to comply

#### Follow Glenn Greenwald by email Stre

the bugg Geen Greenwald, Ewen MacAshill, Laura Poltras. Spencer Ackerman and 07 docum Dominic Rushe graph. Ga The Guardian, Thursday 11 July 2013 Clume to commarks (4174).



Stype worked with intelligence agencies last year to allow Prism to collect video and audio conversations. Photograph: Patrick Sinkel/AP

Microsoft has collaborated closely with US intelligence services to allow users' communications to be intercepted, including helping the National Security Agency to iccrument the company's own encryption, according to top-secret documents obtained by the Guardian.



News US World Sports Comment Culture Business Money



brough covert partnerships with tech companies, the spy agencies have inserted acret vulnerabilities into encryption software. Photograph: Kacher PempatiReuters





Laura Poitras

### See the movie!

### Read the news!



A new bill introduced in Congress gets encryption right.

y

f

g+

00

The bipartisan Secure Data Act would stop any government agency or court order from forcing a company to build backdoors into encrypted devices and communications.

This selection poster of legislation reflexts much of what the community of encryption researchers, scientistic, developers, and advantate have explained for theoremical point constructing an assume herefore, for task works, PTC constraints a point of theoremical point of capital HIII to explain why government mandered backdoore to successing the technical challenges and will western computer security for all, stern that the 100 and 120 continue to give on flaved hereicing approaches to the security organisation for "nequinities entryption," set're glot I a see some Congress members are I intening to the experts and taking this Important step to proteet anyone who uses an entrypted device or service.

EIT supports the Secure Data Act, introduced by Representatives Zoe Lofgren (D=CA), Thomas Massis (R=XV), Ted Poe (R=TX), Terry Nadler (D=NV), Ted Lien (D=CA), and Matt Gaetz (R=TL). You can read the full bill here.

## Backdoors



### Mandatory backdoors

https://www.justice.gov/opa/speech/deputyattorney-general-rod-j-rosenstein-deliversremarks-encryption-united-states-naval

### "Manhattan project"

https://www.cbsnews.com/news/democrati c-debate-transcript-clinton-sanders-omalleyin-new-hampshire/

### No backdoors

https://www.apple.com/customer-letter/

https://www.eff.org/deeplinks/2018/05/secu re-data-act-would-stop-backdoors

Just the same debate with newer technology? <u>https://en.wikipedia.org/wiki/Clipper\_chip</u>

# Modern Cryptography

3

# Cryptography is very old...





https://en.wikipedia.org/wiki/Timeline of cryptography

# Pre-modern cryptography

Based mainly on "linguistic" ideas (see next lecture). Ad hoc deploy-then-patch or replace.

Edgar Allen Poe (an amateur cryptographer):



"human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."



## Is this true?



## Modern Cryptography

- Deals with how to formalize and provably achieve desired properties.
- Security proofs for practical schemes are typically reductions... we will see why.
- Steps: Syntax definition, security definition, construction, reduction.

## Secure Channels Revisited

# **Computational Hardness**

# **Provable Security**





# Why is this the Right Approach?

- Ad-hoc design is subject to bug-thenpatch cycle. Very dangerous and costly.
- "Testing is not possible in this setting, there are an infinite number of adversarial strategies.
- Doesn't make sense to try to design a secure encryption scheme without first asking what "secure" even means.



# Why is this the Right Approach?

• Ad-hoc design is subject to bug-thenpatch cycle. Very dangerous and costly.

• Doesn't make sense to try to design a secure encryption scheme without first asking what "secure" even means.