Indiscreet Logs: Diffie-Hellman Backdoors in TLS

Kristen Dorey Nicholas Chang-Fong Aleksander Essex

Western University, Canada

NDSS 2017
February 28, 2017

Discrete logarithms are “easy” in smooth order groups… if you know the factorization of the group order.

What if you don’t know the group order? What if it was hidden somehow?

Discrete logarithms are “easy” in smooth order groups… if you know the factorization of the group order.

What if you don’t know the group order? What if it was hidden somehow?

The discrete logarithm problem *could* be hard. Or it could be easy. So which one is it?

What if it was manufactured to be easy, and only the attacker can tell?

Outline

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

How many did we find?

What **disclosures** did we do?

What can be done to prevent this?

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

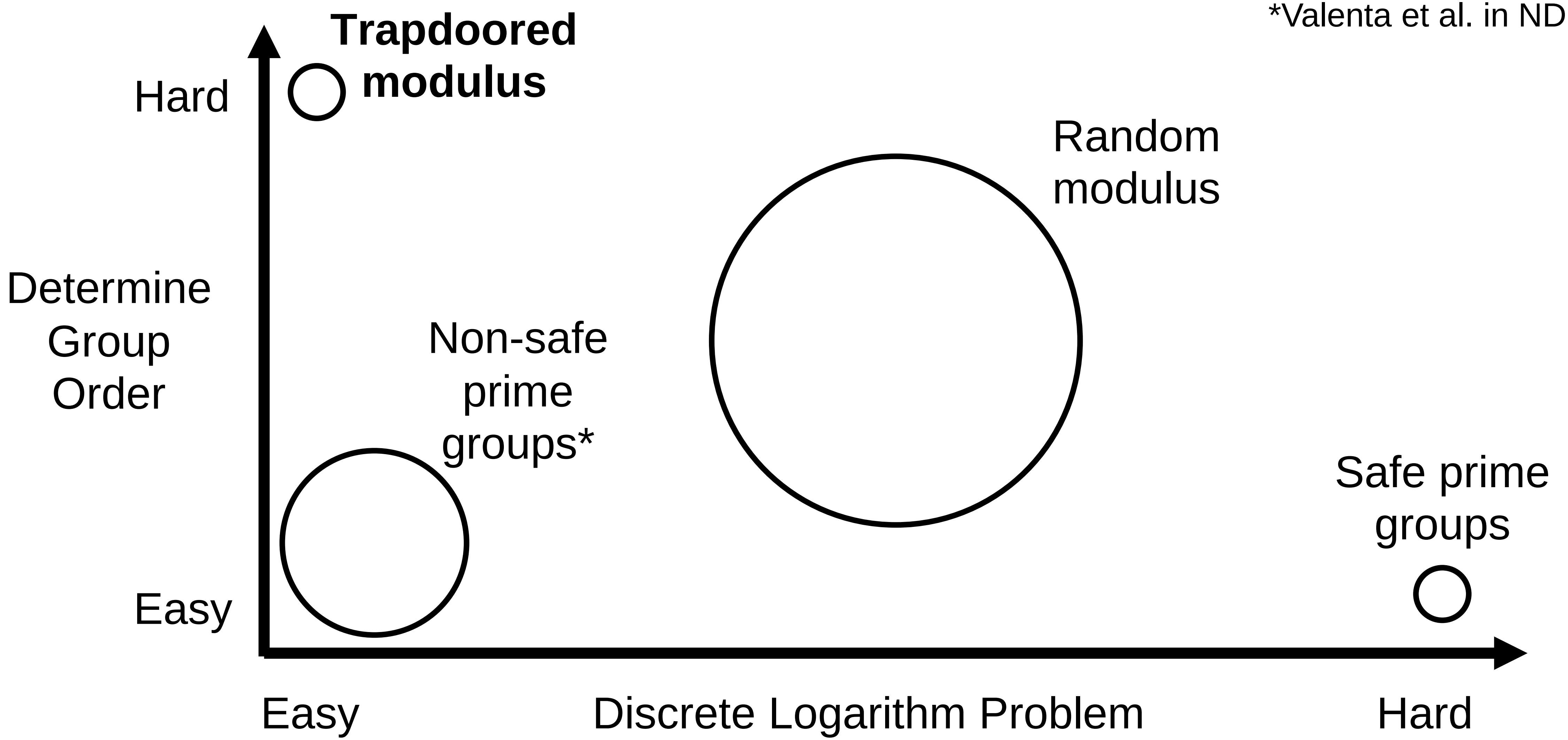
How many did we find?

What **disclosures** did we do?

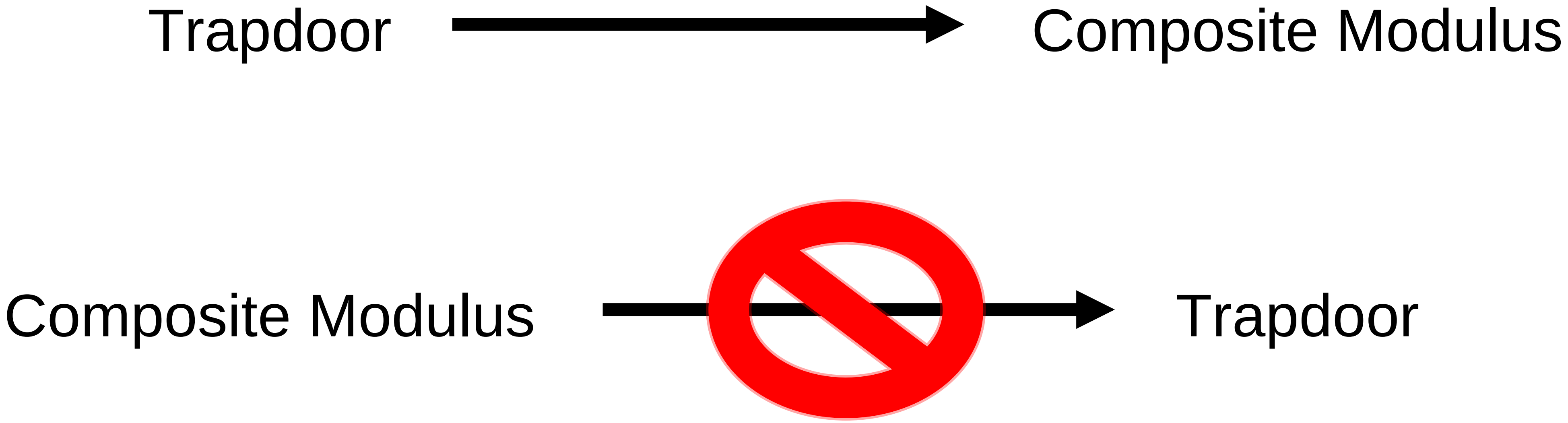
What can be done to prevent this?

Exploiting Small and Smooth Order Subgroups

*Valenta et al. in NDSS 2017



Trapdoor → Composite Modulus



Trapdoor

Composite Modulus

Composite Modulus

Trapdoor

Composite Modulus:

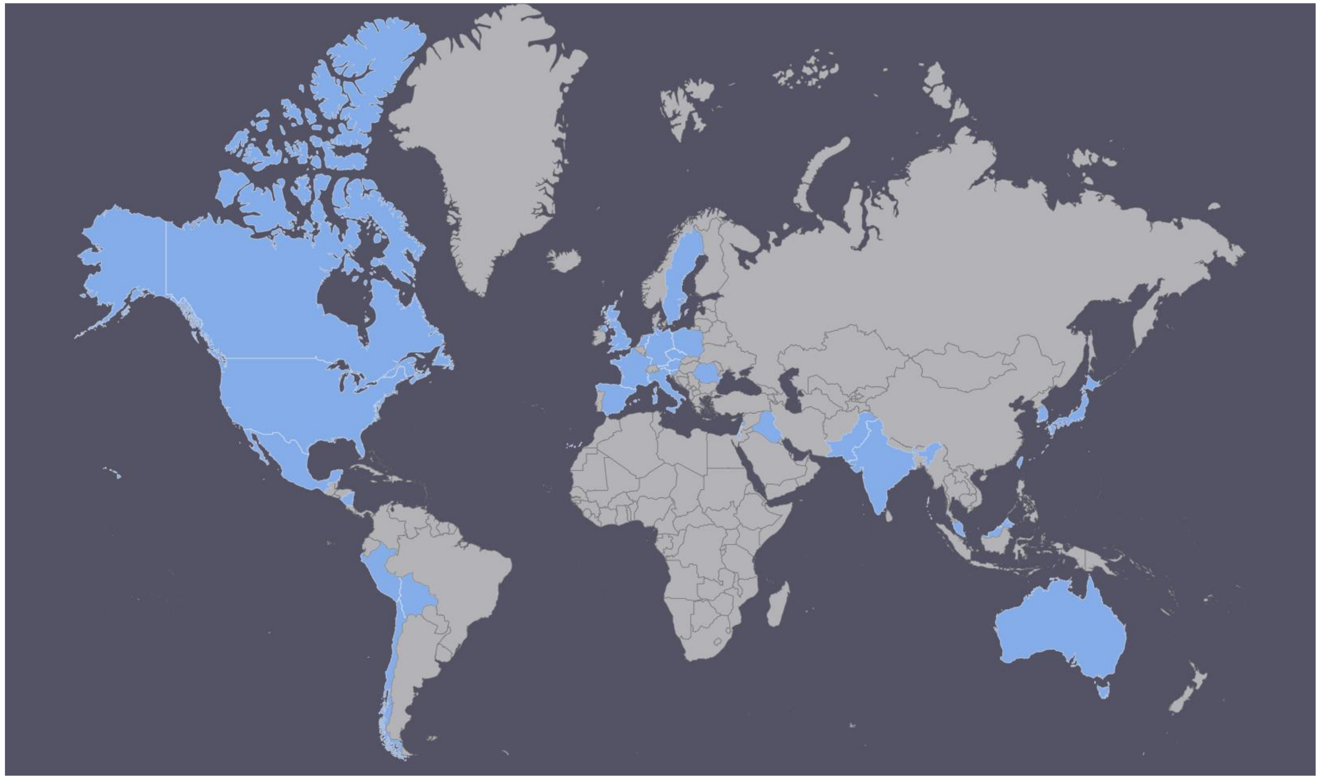
Mistake…or trapdoor?

Can’t tell unless you factor modulus

Vulnerability

The Vulnerability

- Composite DH moduli used in TLS and STARTTLS
- 30+ countries
- 20+ companies



Implications of Trapdoors

- Shared secret recovery
- Passive eavesdropping
- Traffic modification

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

How many did we find?

What **disclosures** did we do?

What can be done to prevent this?

How Is This Possible?

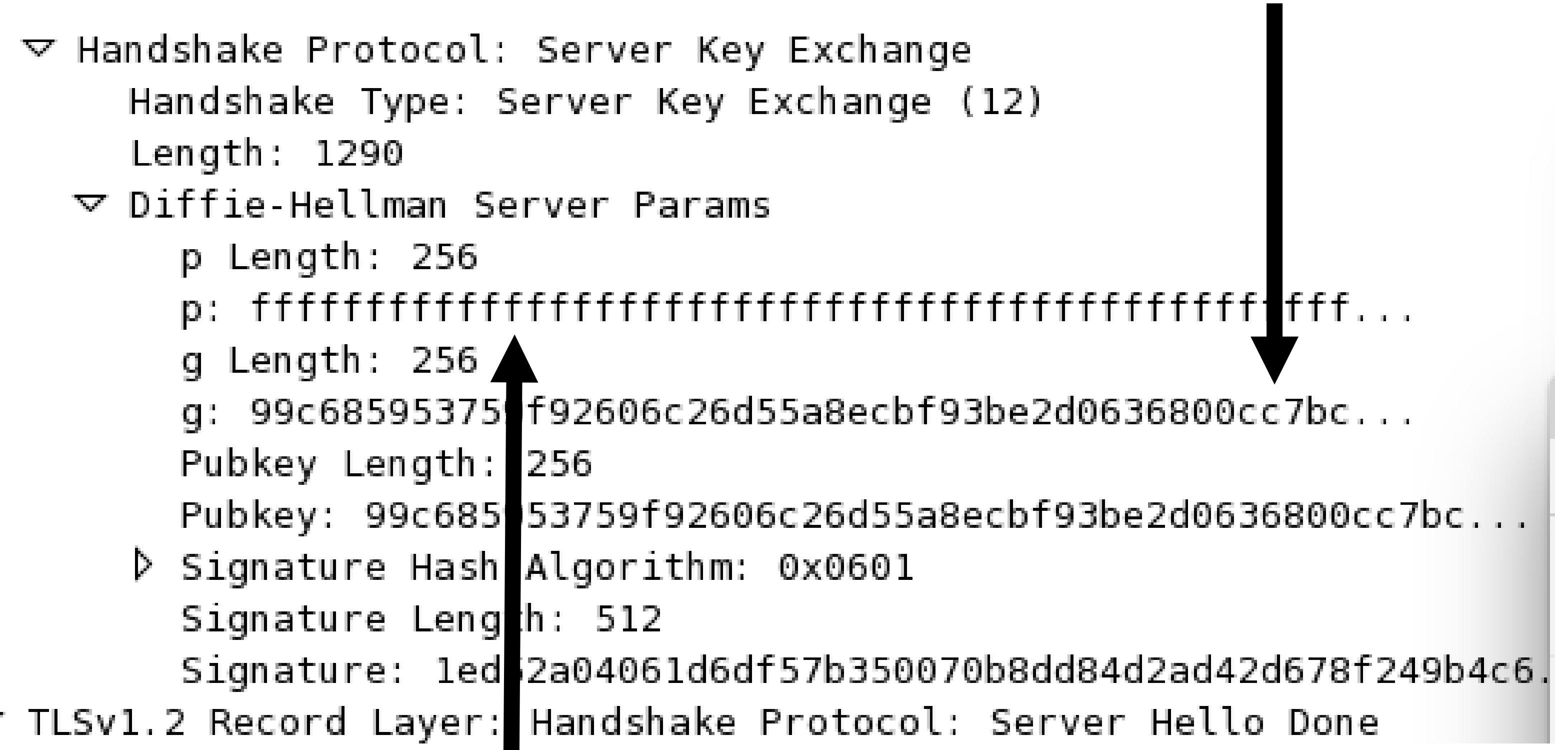
Systematically poor parameter validation by discrete logarithm implementations

Primality not checked
Why not?

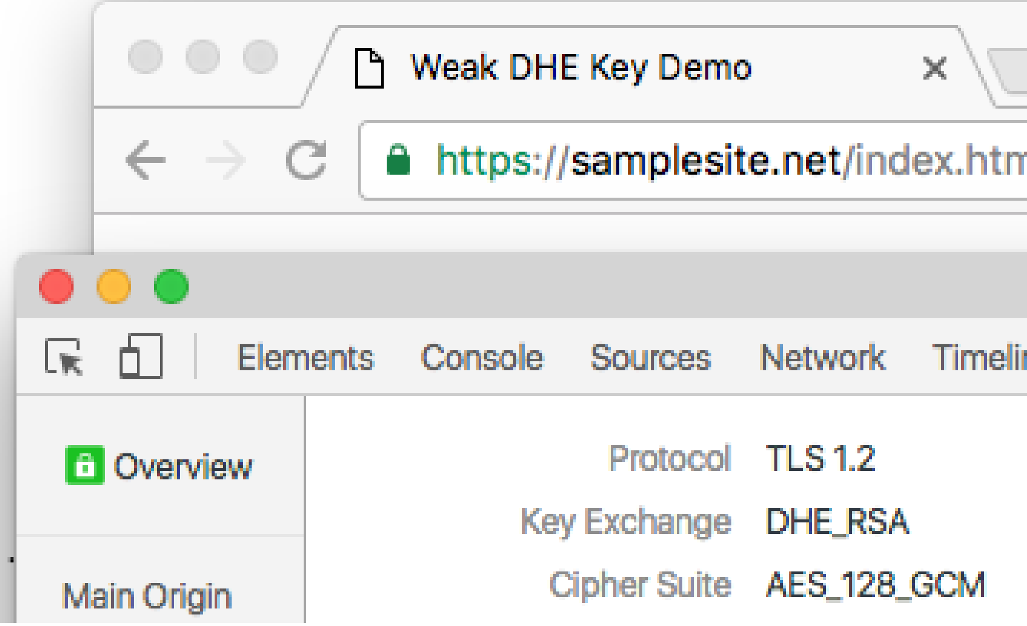
Primality testing is “math fast” but not “Internet fast”

Chrome Connection

Subgroup of order 3



```
▽ Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 1290
  ▽ Diffie-Hellman Server Params
      p Length: 256
      p: ffffffffffffffffffffffffffffffffffffffffffff fff...
      g Length: 256
      g: 99c68595375 f92606c26d55a8ecbf93be2d0636800cc7bc...
      Pubkey Length: 256
      Pubkey: 99c685 53759f92606c26d55a8ecbf93be2d0636800cc7bc...
    ▷ Signature Hash Algorithm: 0x0601
      Signature Length: 512
      Signature: 1ed 2a04061d6df57b350070b8dd84d2ad42d678f249b4c6.
 TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```



Protocol TLS 1.2

Key Exchange DHE_RSA

Cipher Suite AES_128_GCM

Not prime

Private Key = 1

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

How many did we find?

What **disclosures** did we do?

What can be done to prevent this?

Forcing DHE

DHE used in <1% TLS connections but still (somewhat) widely supported

Small subgroups allow attacker to compute master secret

“Downgrade” attack to force DHE ciphersuites for TLS 1.2 and below

Downgrade protections in TLS 1.3 prevent this attack

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

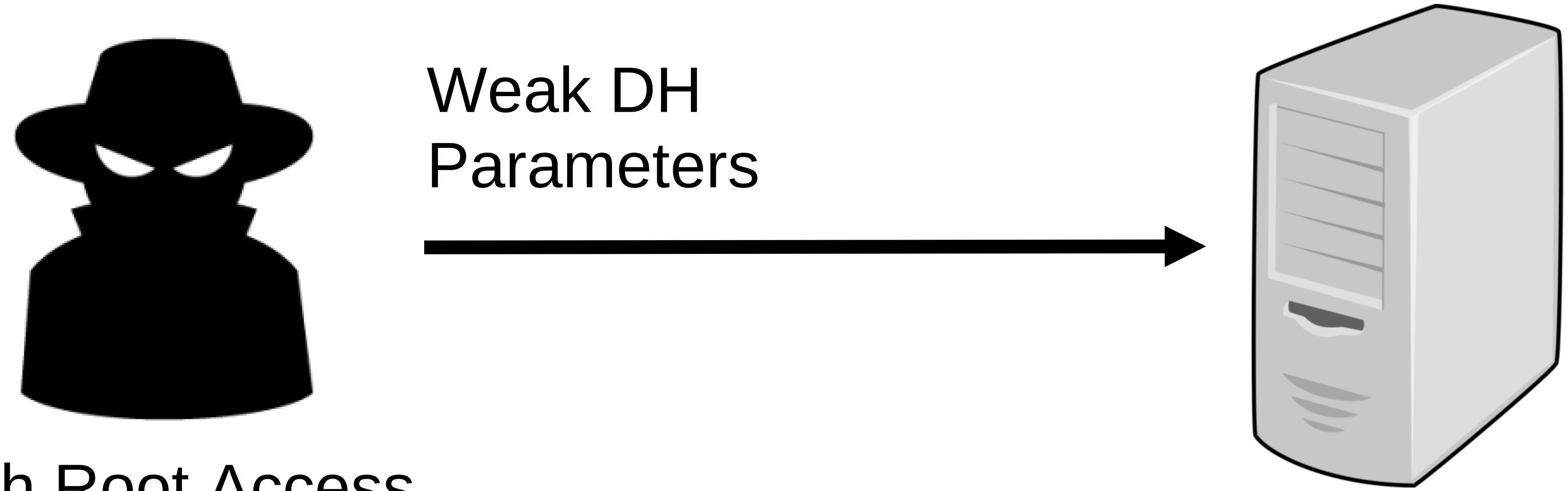
How many did we find?

What **disclosures** did we do?

What can be done to prevent this?

Getting Weak Parameters Used Three attack vectors

1. Drop onto server

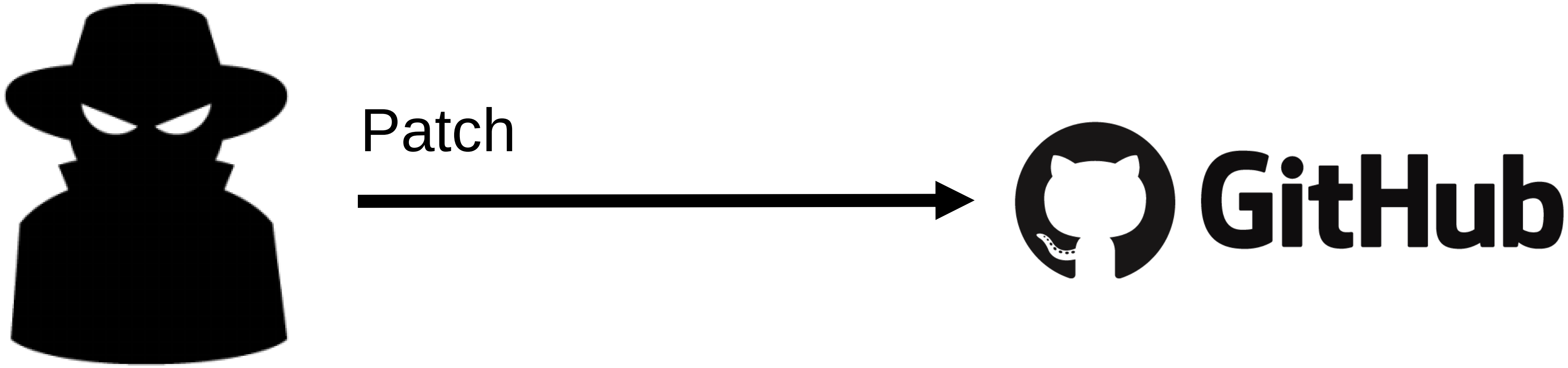


Weak DH Parameters

With Root Access

Getting Weak Parameters Used Three attack vectors

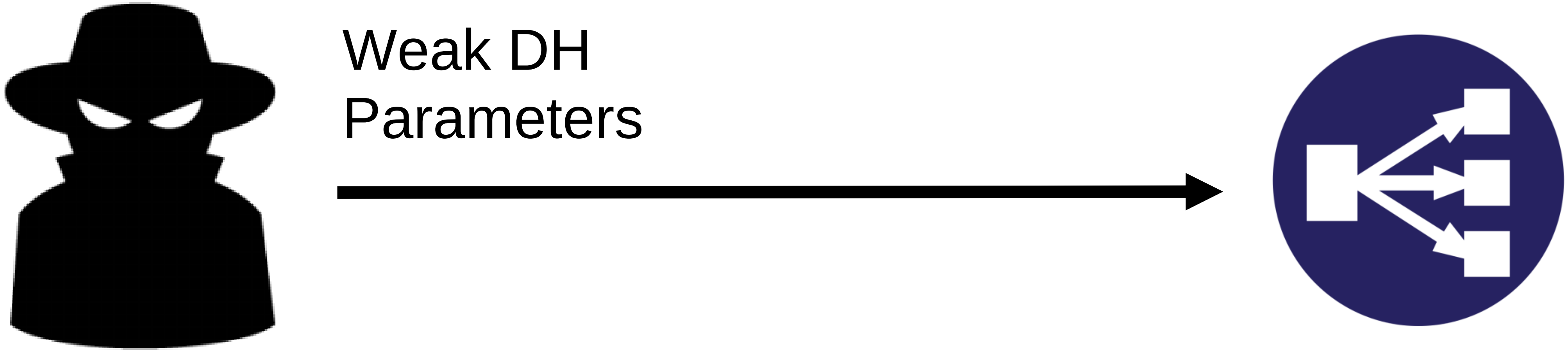
2. Incorporate into open-source project



Patch

Getting Weak Parameters Used Three attack vectors

3. Install onto network appliance before shipment



Weak DH Parameters

Company Employee

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

How many did we find?

What **disclosures** did we do?

What can be done to prevent this?

How Many Weak Parameters Did We Find?

43M IPs using HTTPS, 11M supporting DH

Composite Moduli

- 280 IPs in HTTPS
- 272 IPs in IMAPS, POP3S, SMTPS, SMTP
- Private key recoveries up to 42% of length

How Many Weak Parameters Did We Find?

43M IPs using HTTPS, 11M supporting DH

Composite Moduli

- 280 IPs in HTTPS
- 272 IPs in IMAPS, POP3S, SMTPS, SMTP
- Private key recoveries up to 42% of length

Non-safe Prime Moduli*

- 1.6M IPs in HTTPS
- Private key recoveries up to 50% of length

*Valenta et al. in NDSS 2017

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

How many did we find?

What **disclosures** did we do?

What can be done to prevent this?

Disclosures

BLUE COAT
Expedia
ELITE
FTSE Russell
UNED
SANTA CLARA UNIVERSITY 1851
Universal Sompo General Insurance Co. Ltd.
travel tainment the amadeus leisure group
UPS
KDS
NH HOTEL GROUP
Bloomberg
Nordea
Eyou.net
DER Touristik
A1
JAMF software

Companies

- 56% fixed vulnerability
- 19% in progress
- 25% unchanged

Solutions

- Change to prime moduli
- Remove DHE ciphersuites

What is the **vulnerability**?

How is it **possible**?

How do we **force DH** use?

What are the **attack vectors**?

How many did we find?

What **disclosures** did we do?

What can be done to prevent this?

How Do We Stop It From Occurring?

- Deprecating DH ciphersuites

- Verifying DH parameters correctly
- Use named parameters like for ECDHE
- Sign all previously exchanged messages in ServerKeyExchange

Takeaway Points

Composite moduli of unknown order exist on the Internet today

Could be trapdoored moduli allowing man-in-the-middle attacks, or could just be benign carelessness

We can’t tell and they can’t say

Thank You!
Questions?

WHISPER
LAB.org