Building & Teaching Secure Systems

Andrew Paverd

University of Surrey

12th June 2017

Security Vulnerabilities in Web Technologies

Andrew Paverd

Learning objectives

1. What are web vulnerabilities?

2. Why do they exist?

3. How to mitigate them?

http://ajpaverd.org/teaching/Paverd_Surrey_20170612.pdf

Web vulnerabilities

Security vulnerabilities arising as a consequence of using web technologies

As distinct from:

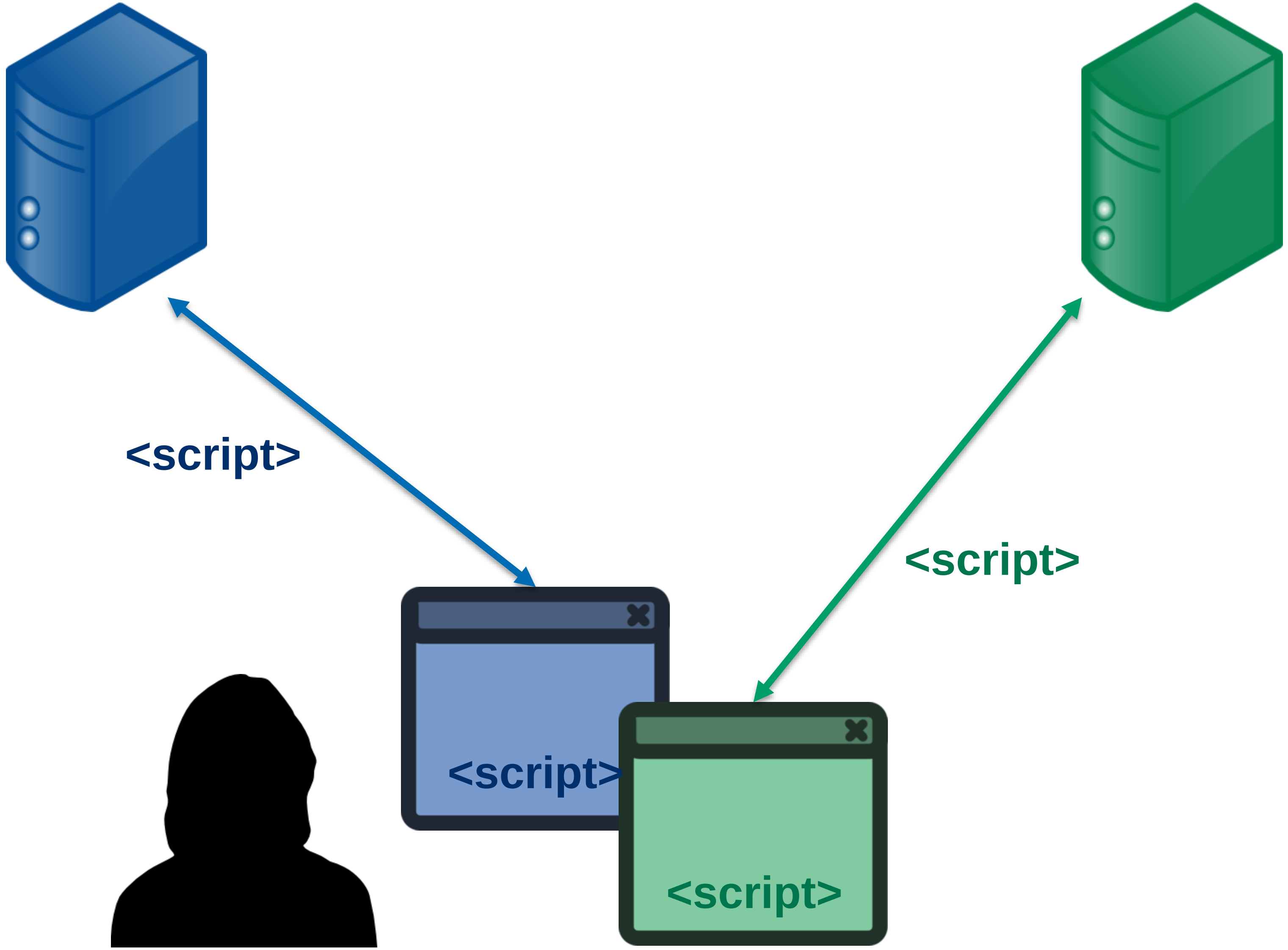
- Flaws in cryptographic algorithms
- Flaws in cryptographic protocols
- Vulnerabilities in platform software (client or server)
- Vulnerabilities in network infrastructure

OWASP Top 10 *(2013)*

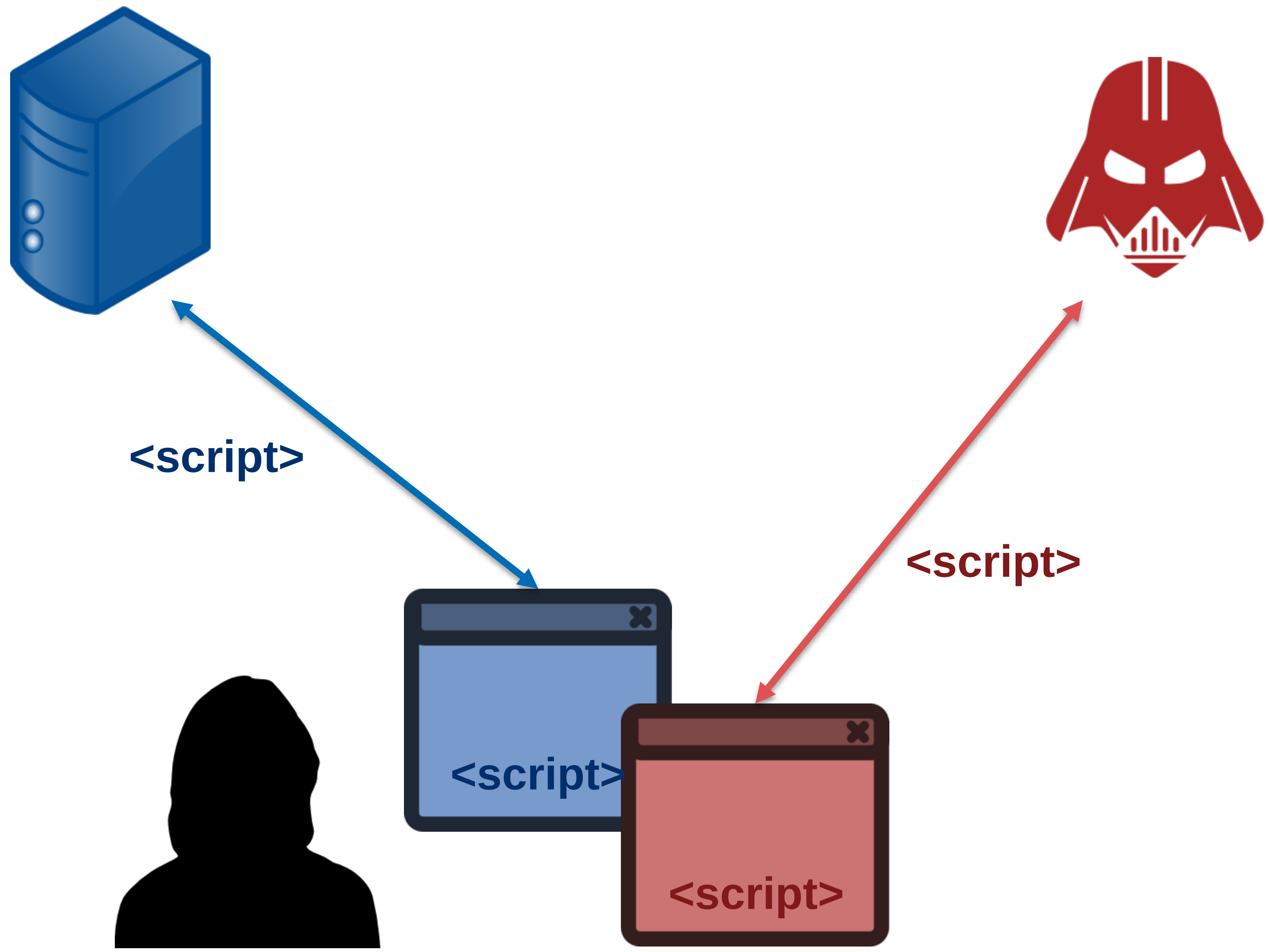
A1	Injection
A2	Broken Authentication and Session Management
A3	Cross-Site Scripting (XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Function Level Access Control
A8	Cross-Site Request Forgery (CSRF)
A9	Using Components with Known Vulnerabilities
A10	Unvalidated Redirects and Forwards

Open Web Application Security Project (OWASP) Top 10 (2013)
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013

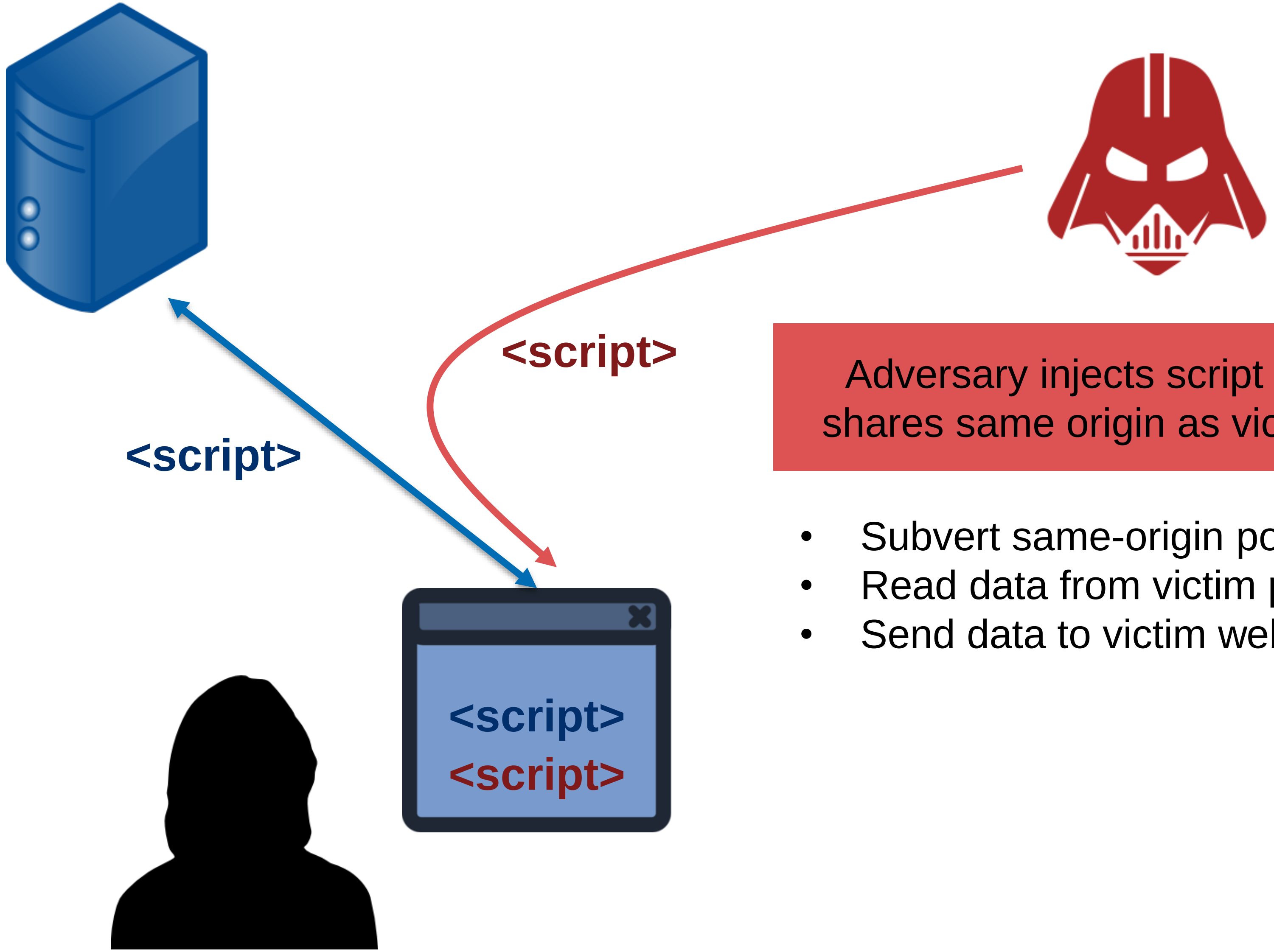
Same-origin policy



Same-origin policy



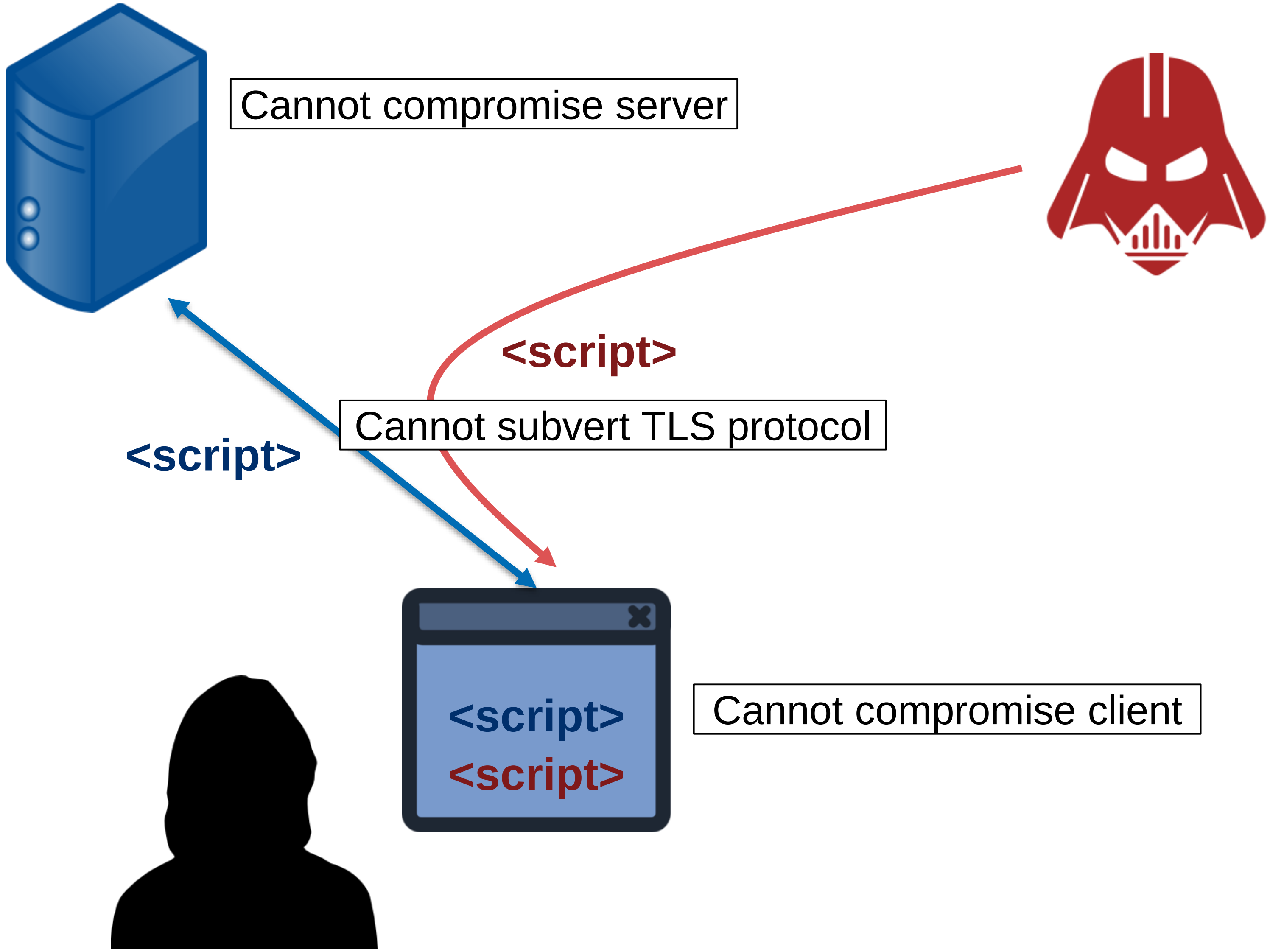
Adversary's Goal



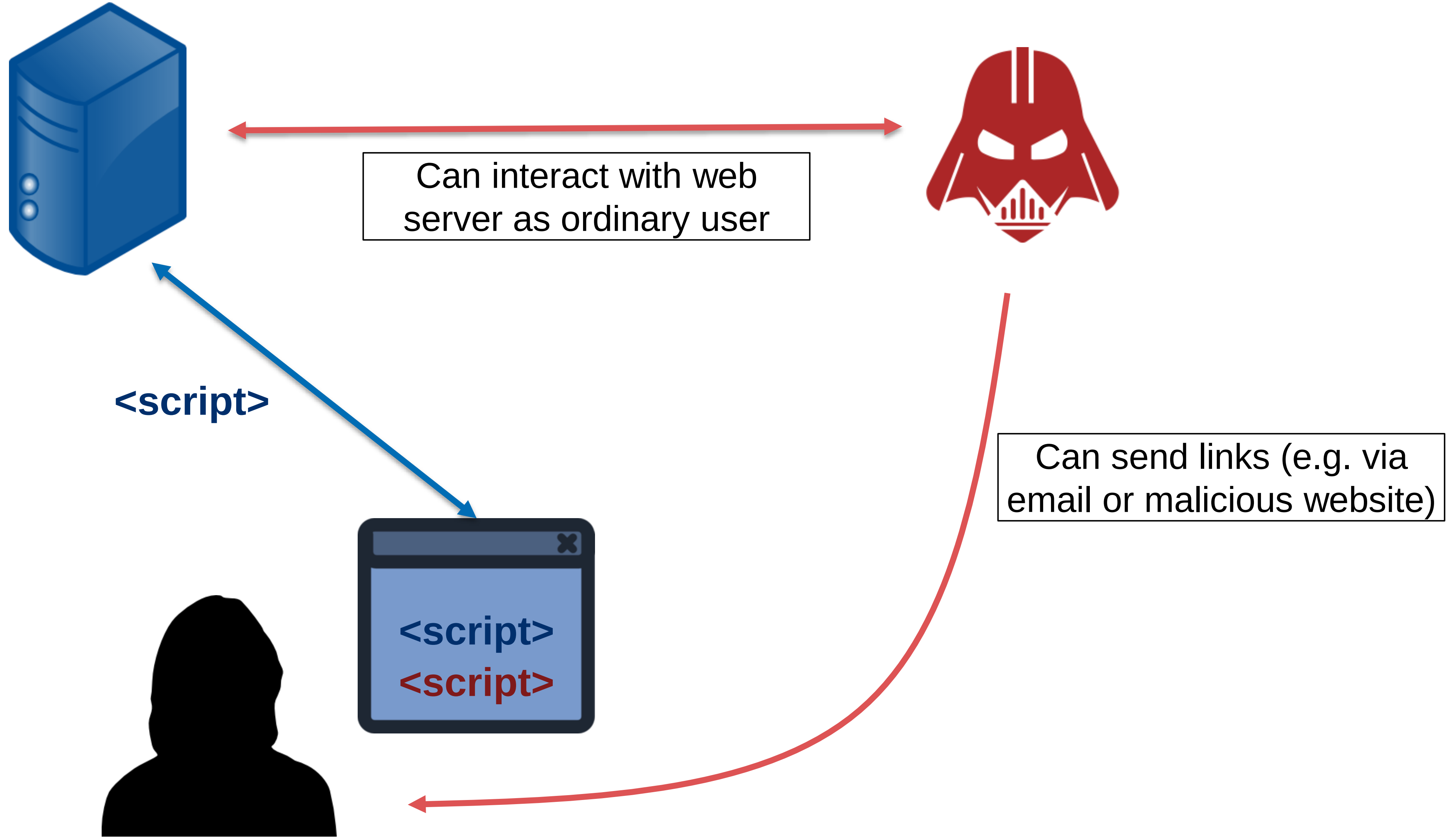
Adversary injects script such that it shares same origin as victim website.

- Subvert same-origin policy
- Read data from victim page
- Send data to victim website

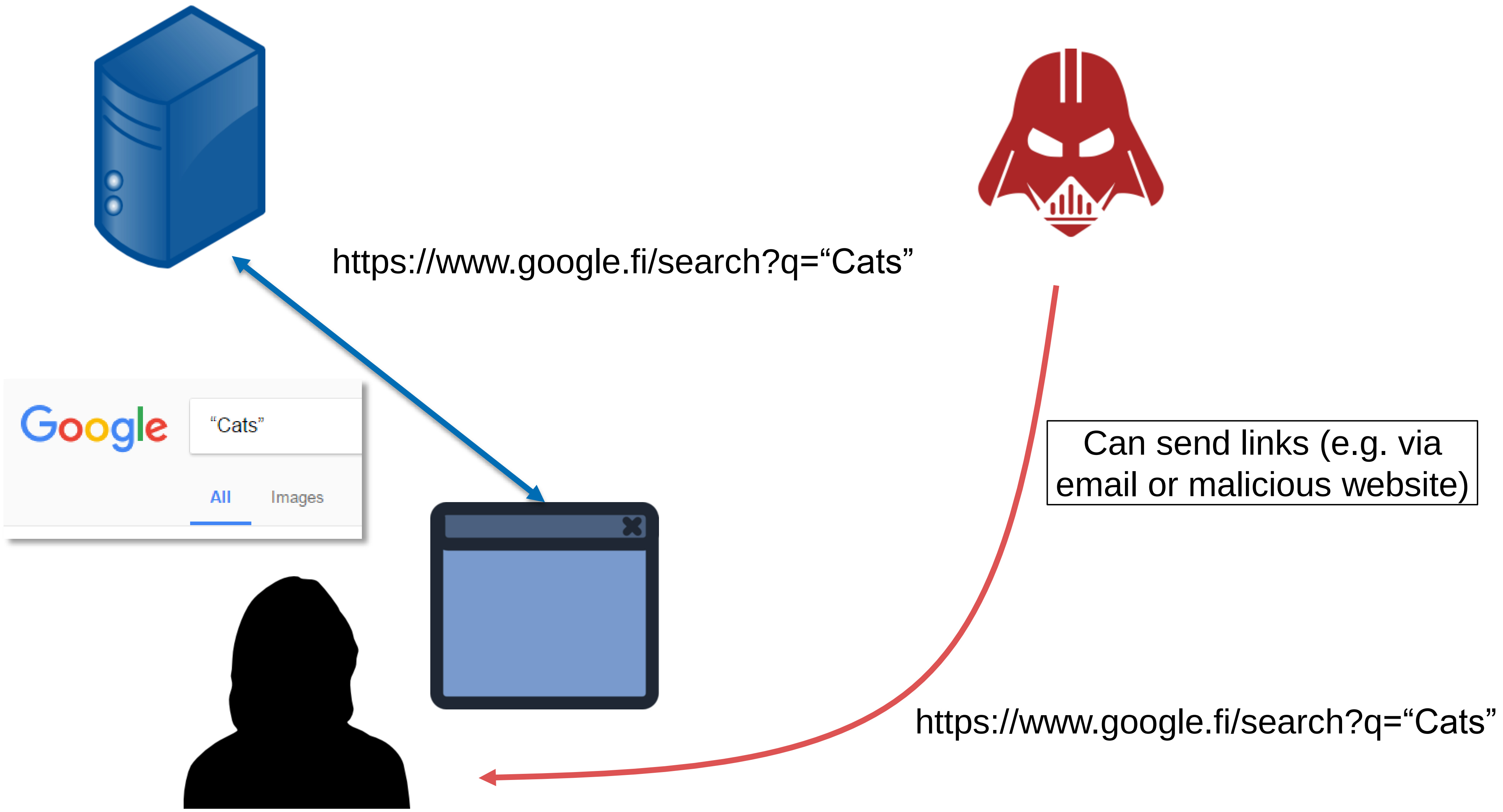
Adversary’s Capabilities



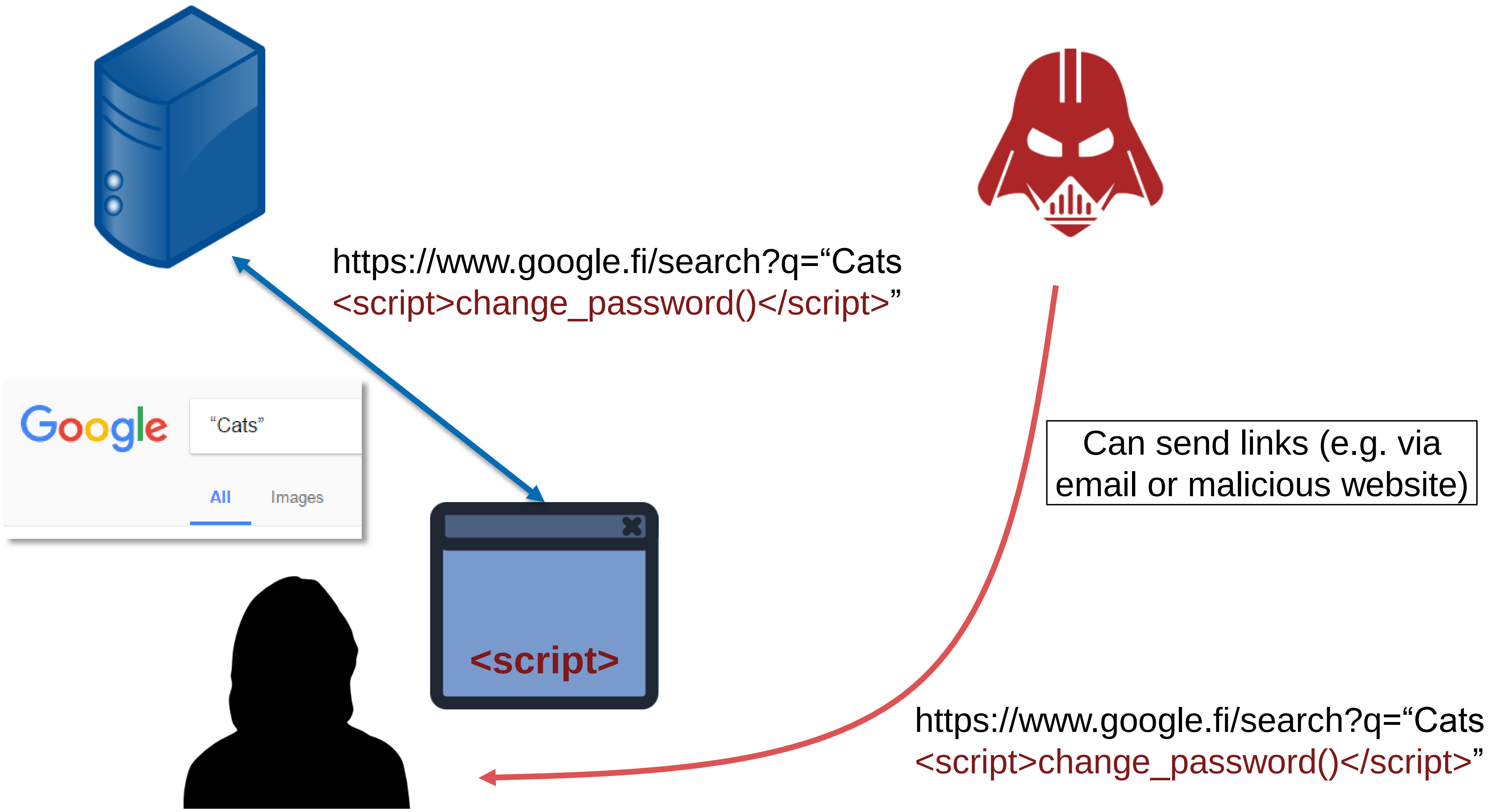
Adversary’s Capabilities



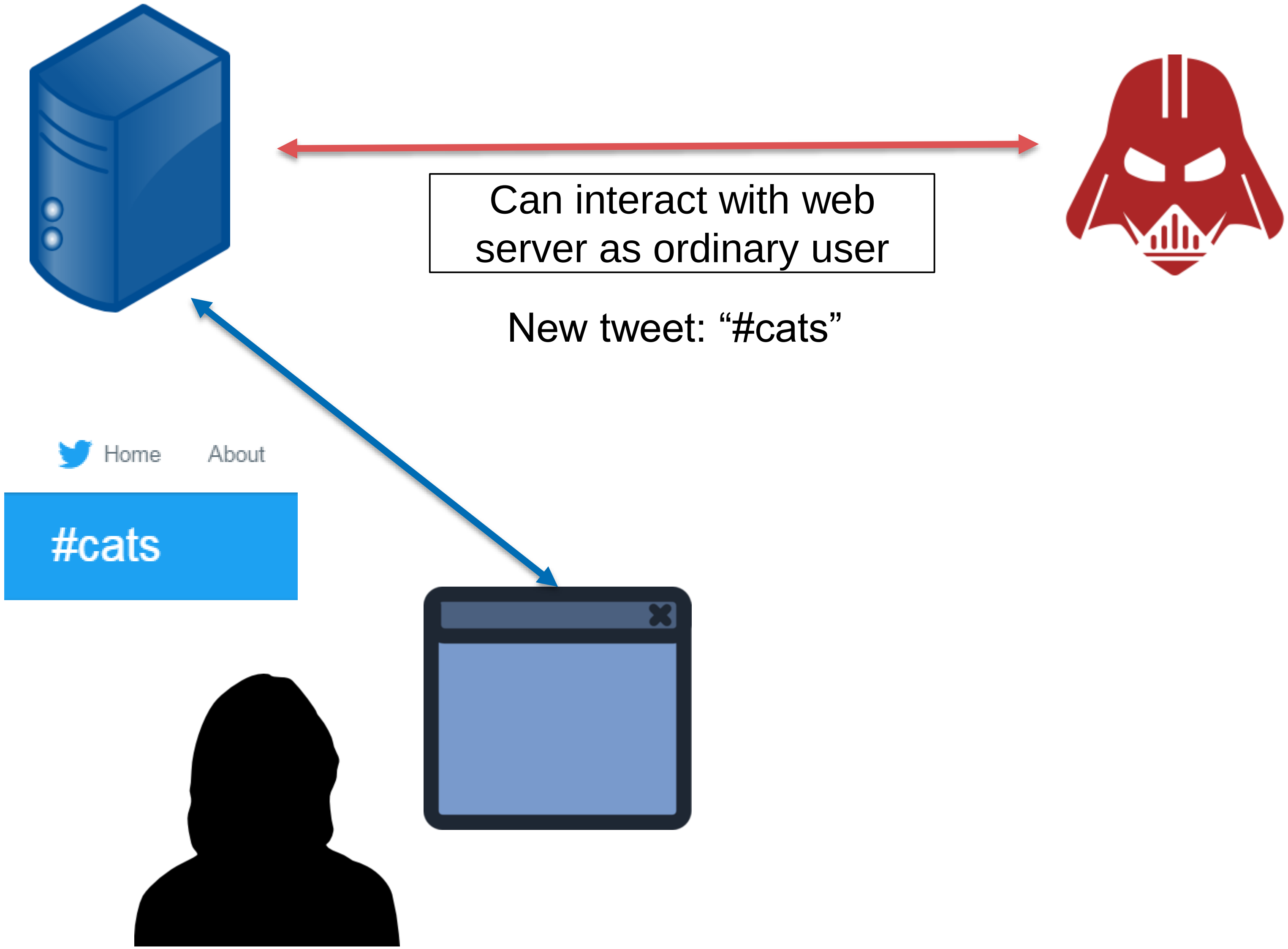
Adversary’s Capabilities



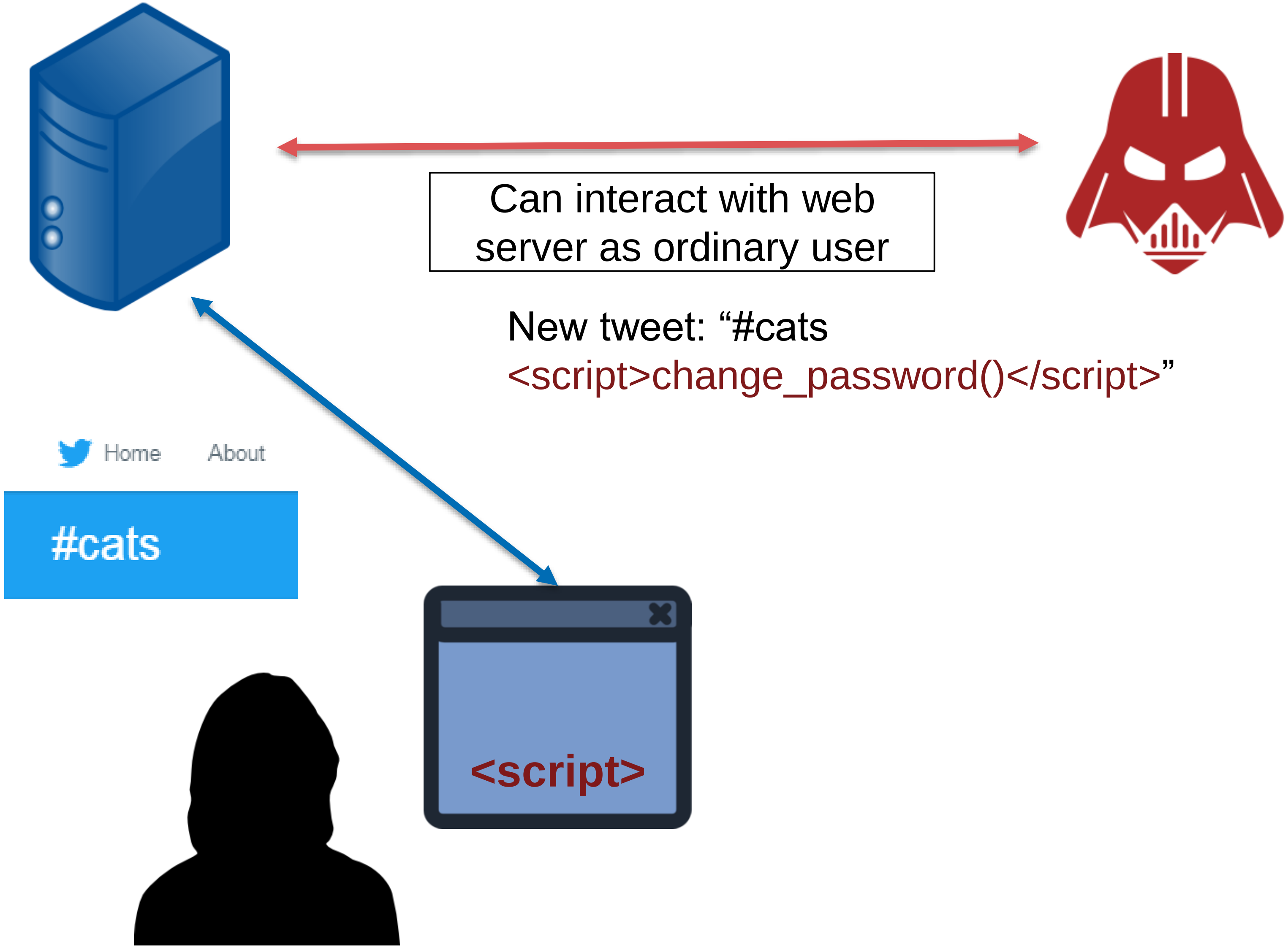
Reflected cross-site scripting (XSS)



Adversary’s Capabilities



Persistent XSS



What went wrong (XSS)?

1. **Adversary supplies payload script to server**
    - e.g. via URL or post on server

2. **Server sends payload to client**
    - No input sanitization
    - Incorrect HTML/script escaping

3. **Client executes payload as if it originated from server**

Mitigating XSS

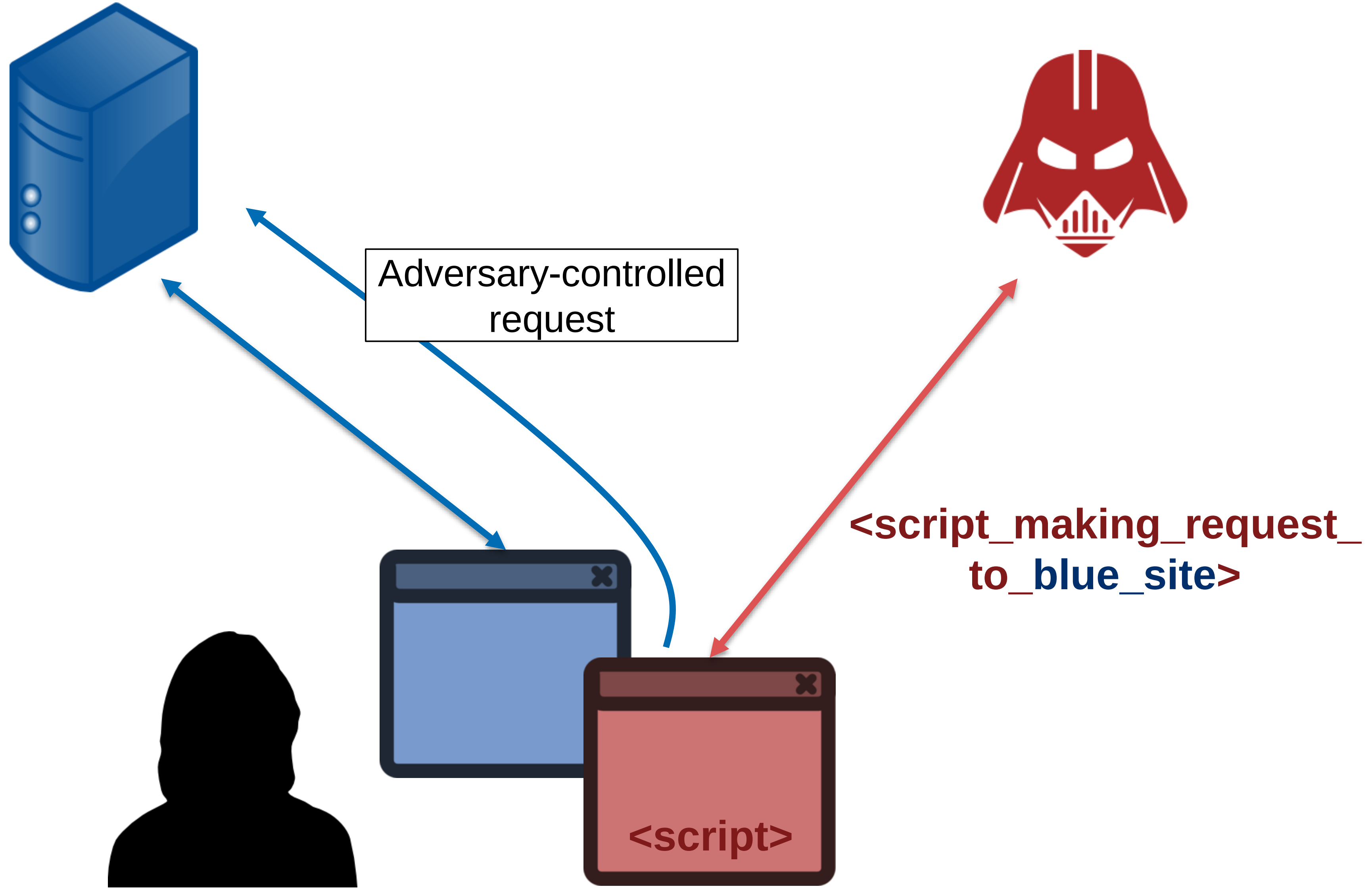
1. **Adversary supplies payload script to server**
   - e.g. via URL or post on server

2. **Server sends payload to client**
   - No input sanitization
   - Incorrect HTML/script escaping

3. **Client executes payload as if it originated from server**

- **Server can reject user-supplied HTML/scripts**
- **Server can ensure all user-supplied content is properly escaped.**

For comparison: Cross-site request forgery (CSRF)



What went wrong (XSRF)?

1. **Adversary supplies payload script to client**
   - e.g. via a malicious page

2. **Client executes payload and sends request to server**
   - Domain name looks innocent
   - Related to a different site

3. **Server processes request as if it originated from client**
   - Server trusts the browser

Mitigating XSRF

1. **Adversary supplies payload script to client**
   - e.g. via a malicious page

2. **Client executes payload and sends request to server**
   - Domain name looks innocent
   - Related to a different site

- **Difficult to change client behaviour**

3. **Server processes request as if it originated from client**
   - Server trusts the browser

- **Additional authentication data in every request (e.g. synchronizer token pattern)**

Research advances

Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense

Yacin Nadji*
Illinois Institute of Technology
Chicago, IL, USA
yacin@ir.iit.edu

Prateek Saxena
University of California
Berkeley, CA, USA
prateeks@eecs.berkeley.edu

Dawn Song
University of California
Berkeley, CA, USA
dawnsong@cs.berkeley.edu

Abstract

Cross-site scripting (or XSS) has been the most dominant class of web vulnerabilities in 2007. The main underlying reason for XSS vulnerabilities is that web markup and client-side languages do not provide principled mechanisms to ensure secure, ground-up isolation of user-generated data in web application code. In this paper, we develop a new approach that combines randomization of web application code and runtime tracking of untrusted data both on the server and the browser to combat XSS attacks. Our technique ensures a fundamental integrity property that prevents untrusted data from altering the structure of trusted code throughout the execution lifetime of the web application. We call this property document structure integrity *(or DSI). Similar to prepared statements in SQL, DSI enforcement ensures automatic syntactic isolation of inline user-generated data at the parser-level. This forms the basis for confinement of untrusted data in the web browser based on a server-specified policy.*

tional vulnerabilities observed in that period [37]. Web Application Security Consortium's XSS vulnerability report shows that over 30% of the web sites analyzed in 2007 were vulnerable to XSS attacks [43]. In addition, there exist publicly available XSS attack repositories where new attacks are being added constantly [44].

Web languages, such as HTML, have evolved from lightweight mechanisms for static data markup, to full blown vehicles for supporting dynamic code execution of web applications. HTML allows inline constructs both to embed untrusted data and to invoke code in higher-order languages such as JavaScript. Due to their somewhat ad-hoc evolution to support demands of the growing web, HTML and other web languages lack principled mechanisms to separate trusted code from inline data and to further isolate untrusted data (such as user-generated content) from trusted data. As a result, web developers pervasively use fragile input validation and sanitization mechanisms, which have been notoriously hard to get right and have lead to numerous subtle security holes. We make the following observations

Y. Nadji, P. Saxena, D. Song. [Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense](), NDSS 2009.

Did you learn…

1. **What are web vulnerabilities?**
   - OWASP Top 10

2. **Why do they exist?**
   - In-depth example: Same-origin policy and Cross-Site Scripting (XSS)
   - Adversary goals
   - Adversary capabilities
   - For comparison: Cross-Site Request Forgery (XSRF)

3. **How to mitigate them?**
   - Examples: Input sanitization, synchronizer token pattern

http://ajpaverd.org/teaching/Paverd_Surrey_20170612.pdf

Questions?

Research Highlights

Andrew Paverd

Research overview *

Publication abstracts 2011-2017, top 100 words.

Research themes

Trusted computing & remote attestation

- SmartGridSec'12, SmartGridSec'14, IEEE SmartGridComm'14, SysTEX@Middleware'16

Software security

- ACM CCS'16, ACM/IEEE DAC'17

Cloud security & privacy

- SysTEX@Middleware'16, IEEE Internet Computing 2017, ACM ASIACCS'17 *(honourable mention)*

Mobile, embedded & IoT

- HomeSys@UbiComp'14, ACM/IEEE DAC'16, ACM TODAES 2017

Formal methods; blockchains & distributed systems; V2X; technology and law

Research themes & potential collaboration

Trusted computing & remote attestation ***(Chen)***

- SmartGridSec’12, SmartGridSec’14, IEEE SmartGridComm’14, SysTEX@Middleware’16

Software security

- ACM CCS’16, ACM/IEEE DAC’17

Cloud security & privacy ***(Gillam)***

- SysTEX@Middleware’16, IEEE Internet Computing 2017, ACM ASIACCS’17 *(honourable mention)*

Mobile, embedded & IoT ***(Giannetsos)***

- HomeSys@UbiComp’14, ACM/IEEE DAC’16, ACM TODAES 2017

Formal methods; blockchains & distributed systems; V2X; technology and law

(Boureanu, Manulis, Schneider, Treharne, Williams)

Research themes

Trusted computing & remote attestation

- SmartGridSec'12, SmartGridSec'14, IEEE SmartGridComm'14, SysTEX@Middleware'16

Software security

- ACM CCS'16, ACM/IEEE DAC'17

Cloud security & privacy

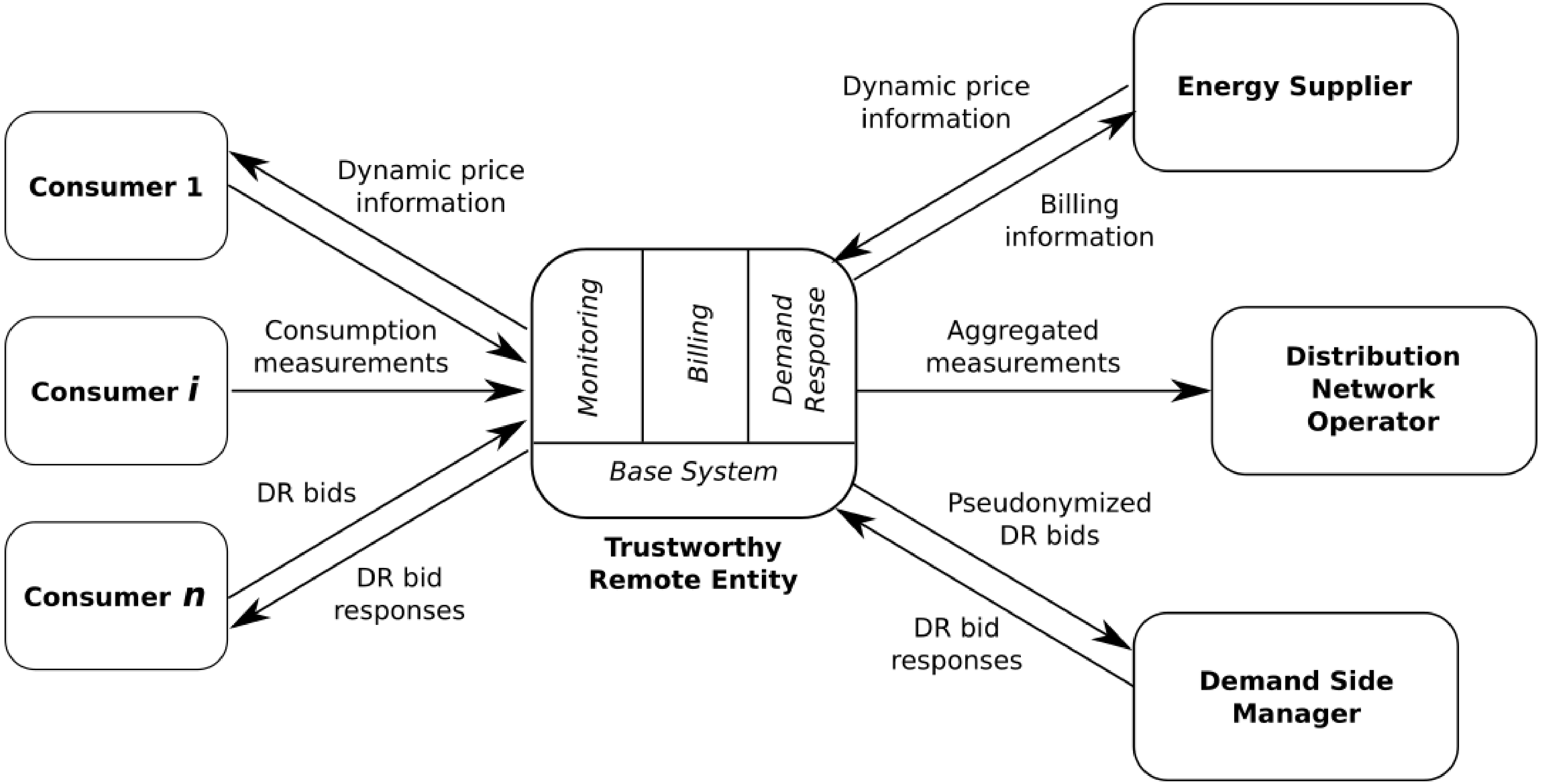
- SysTEX@Middleware'16, IEEE Internet Computing 2017, ACM ASIACCS'17 *(honourable mention)*

Mobile, embedded & IoT

- HomeSys@UbiComp'14, ACM/IEEE DAC'16, ACM TODAES 2017

Formal methods; blockchains & distributed systems; V2X; technology and law

Trustworthy Remote Entities

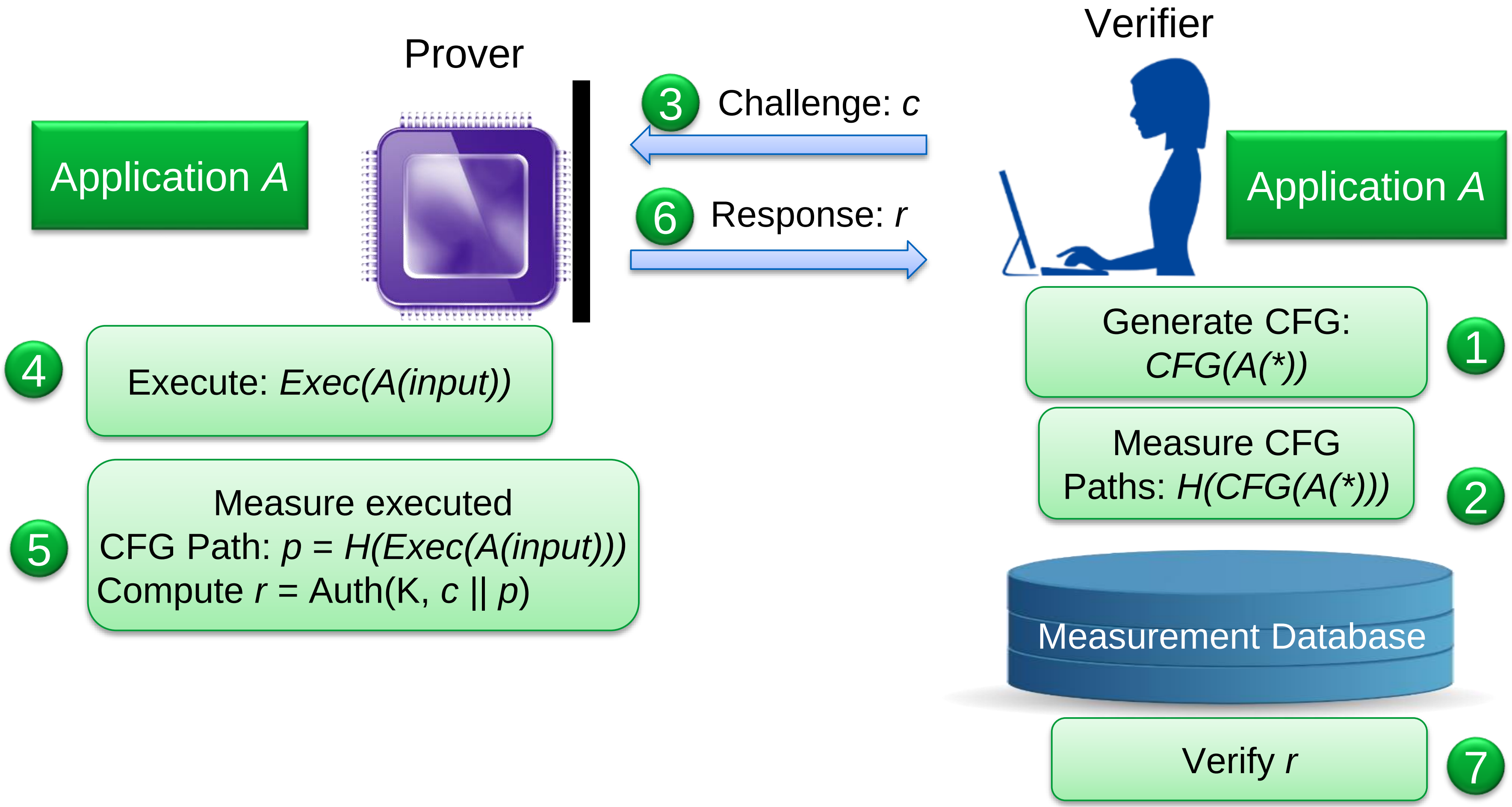


- Smart energy Grid
- Protocol analysis using CSP
- Minimal TCB
- Scalable attestation

Formed the basis for AppTRE project at Oxford (2 PhD studentships), funded by Intel.

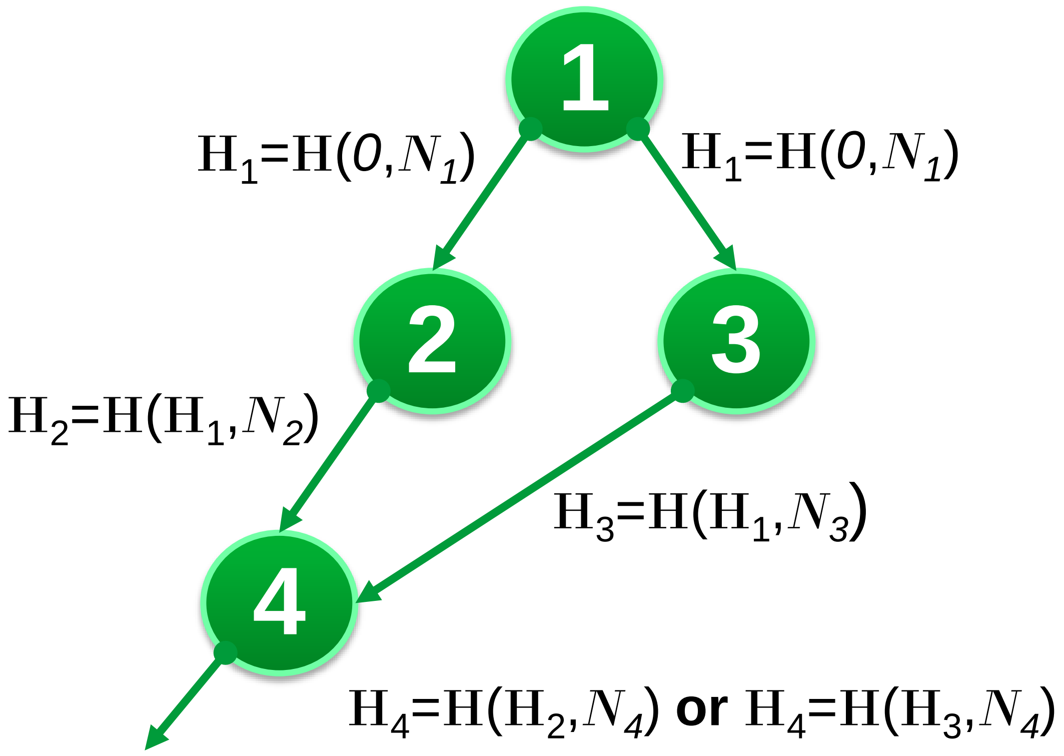
A. Paverd, A. Martin, I. Brown, [Privacy-enhanced bi-directional communication in the Smart Grid using trusted computing](), IEEE Smart Grid Communications (SmartGridComm), 2014.

Control-Flow Attestation



T. Abera, N. Asokan, L. Davi, J-E. Ekberg, T. Nyman, A. Paverd, A-R. Sadeghi, G. Tsudik, *C-FLAT: Control Flow Attestation for Embedded Systems Software*, ACM CCS '16.

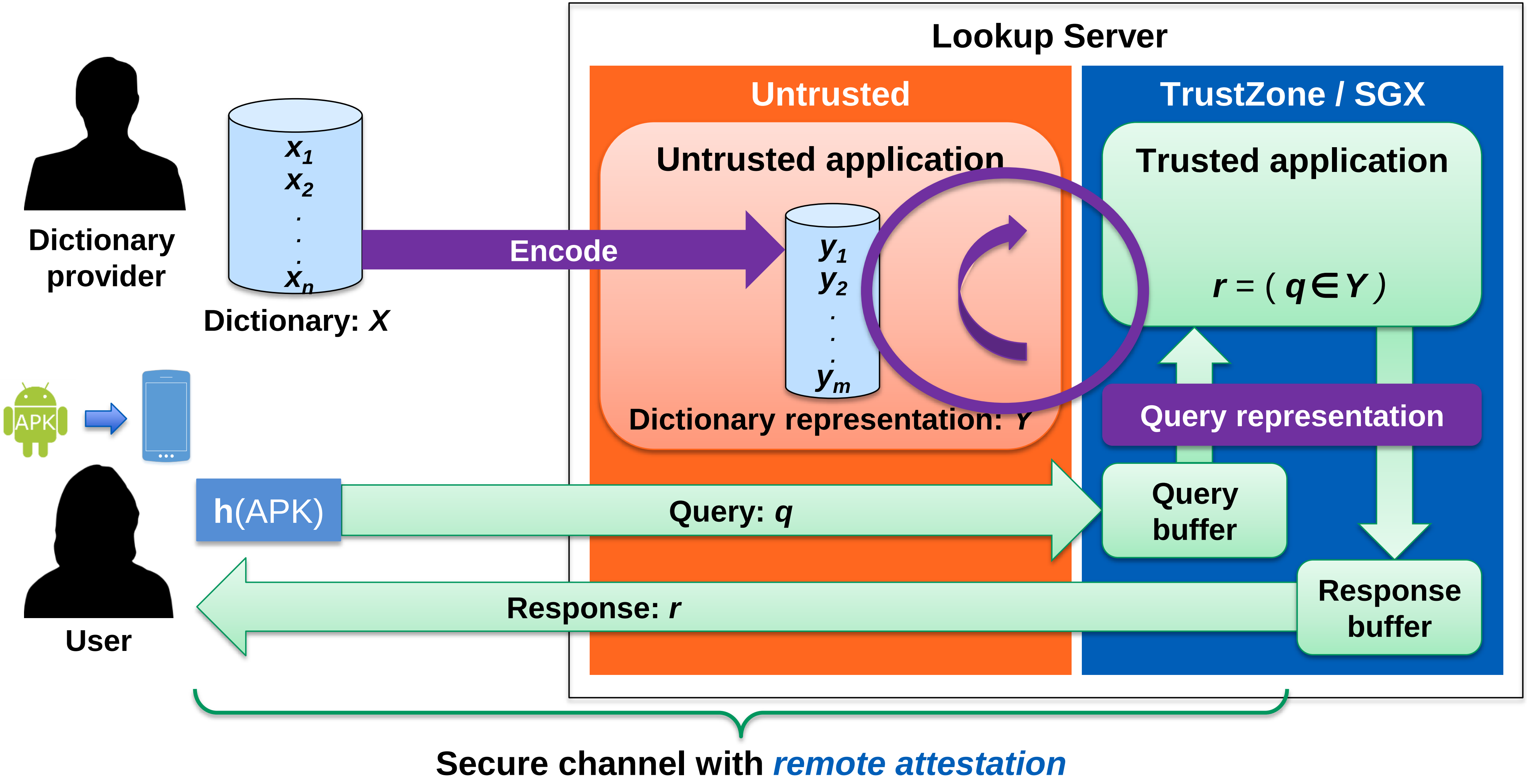
Control-Flow Attestation



Can this be applied to vehicles or critical infrastructure?

T. Abera, N. Asokan, L. Davi, J-E. Ekberg, T. Nyman, A. Paverd, A-R. Sadeghi, G. Tsudik, [C-FLAT: Control Flow Attestation for Embedded Systems Software], ACM CCS '16.

Scalable Private Membership Test



S. Tamrakar, J. Liu, A. Paverd, J-E. Ekberg, B. Pinkas and N. Asokan, The Circle Game: Scalable Private Membership Test Using Trusted Hardware, ACM ASIACCS 2017 (honourable mention)

Future Research

Andrew Paverd

Research principles

1. **Relevant problems**
    - Realistic adversary models
    - Real users

2. **Prototypes are mandatory**
    - Security as an emergent property
    - Accurate performance measurements
    - Reproducibility

3. **Secure + Usable + Deployable**
    - “Who will run the servers?”

Proposed research

Use trusted hardware and remote attestation across the full spectrum of systems to:

1. **Enable new communication paradigms**

2. **Improve energy efficiency**

3. **Support the full system life-cycle**

Supported by: **formal protocol analysis, collaboration with domain experts, collaboration with other disciplines (e.g. law).**

Proposed research

Use trusted hardware and remote attestation across the full spectrum of systems:

Intel SGX
(SysTEX'16 x2,
ASIACCS'17)

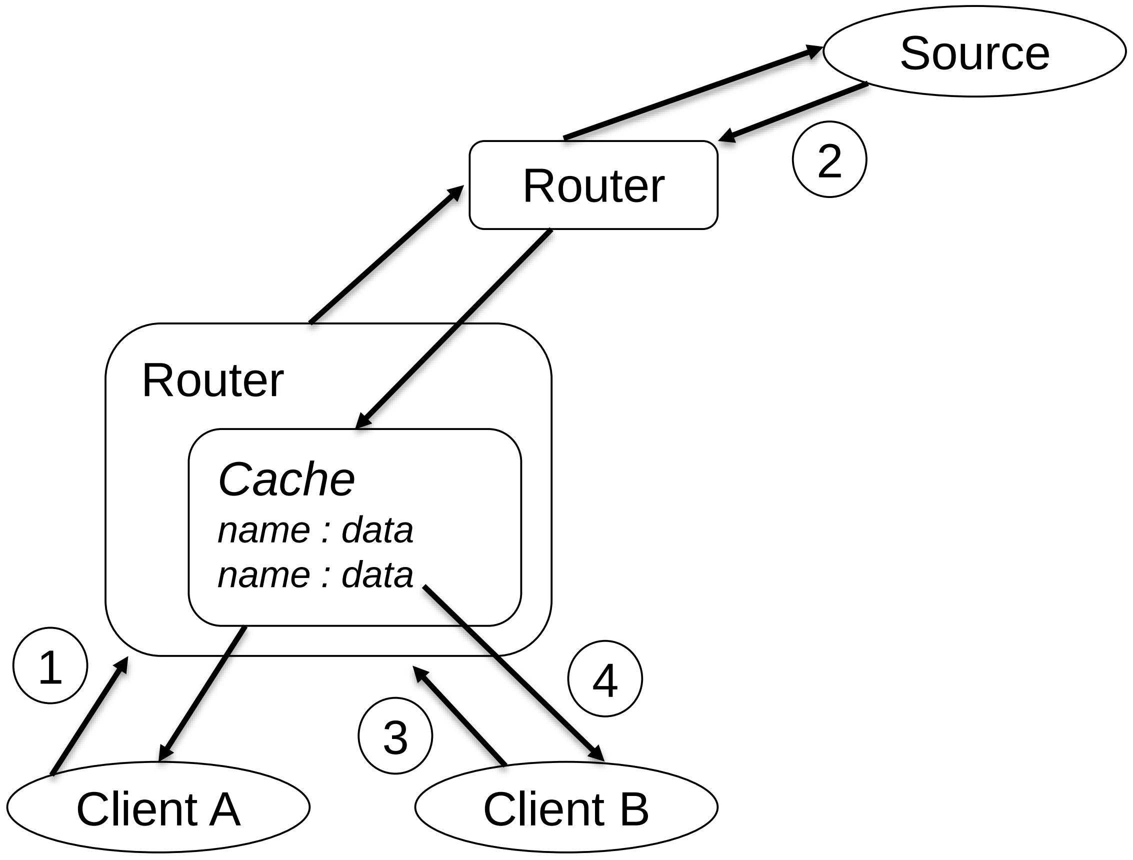
TPM
(SmartGridSec'12,
SmartGridSec'14,
SmartGridComm'14)

ARM TrustZone
(CCS'16,
ASIACCS'17)

Custom hardware
(DAC'17)

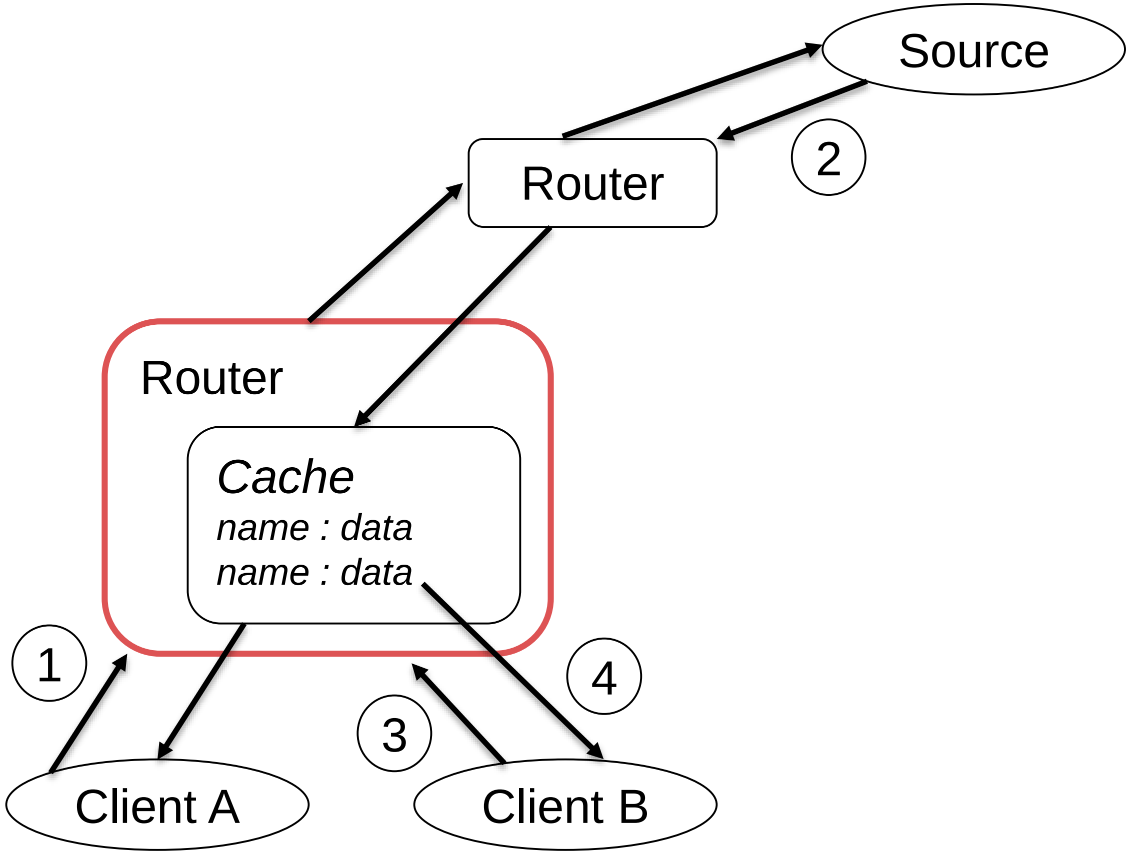
New Communication Paradigms (1)

Information-Centric Networking (ICN)



New Communication Paradigms (1)

Information-Centric Networking (ICN)



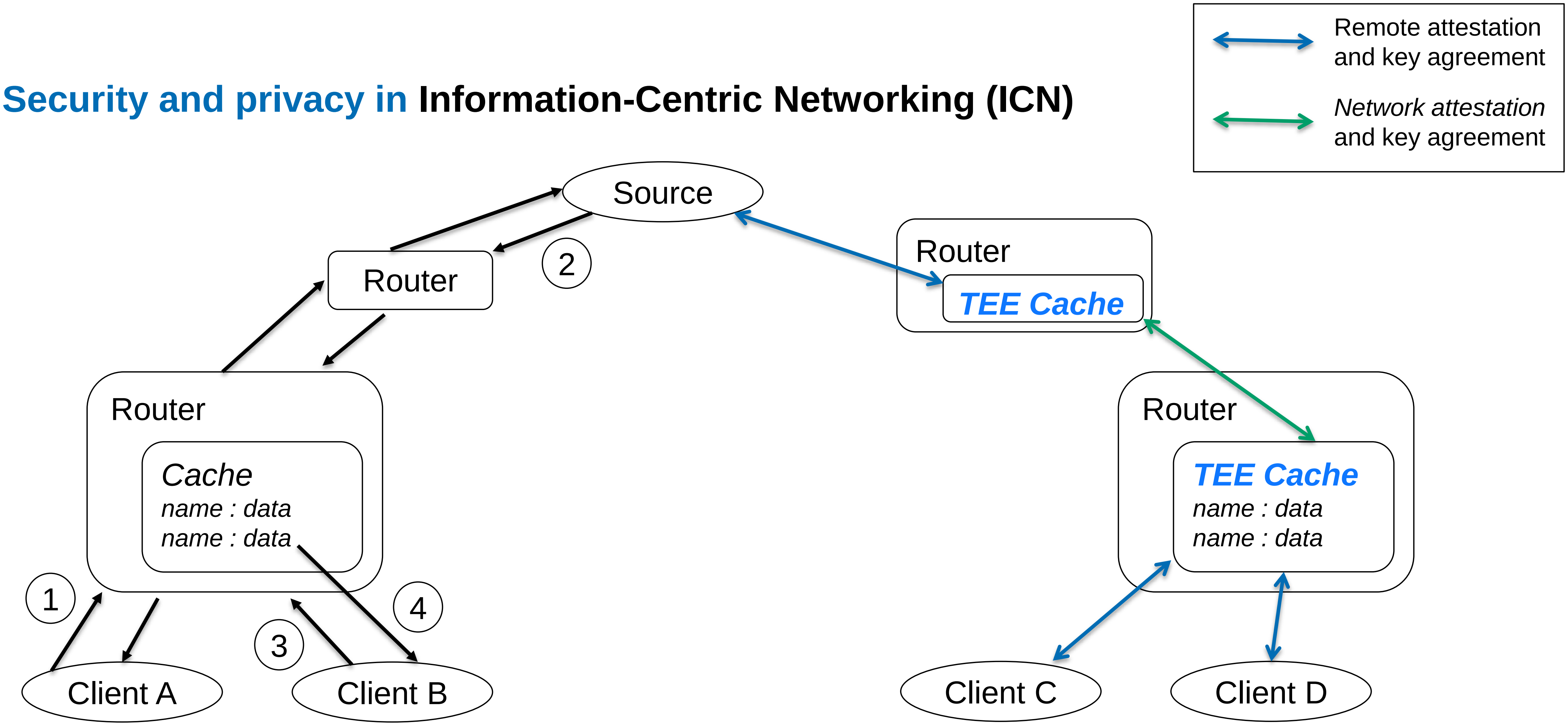
Security guarantees

- Authenticity and integrity through digital signatures
- No confidentiality of requests
- No confidentiality of data
- Information leaks to neighbours

C. Ghali, G. Tsudik, C. Wood, [(The Futility of) Data Privacy in Content-Centric Networking], ACM on Workshop on Privacy in the Electronic Society (WPES), 2016.

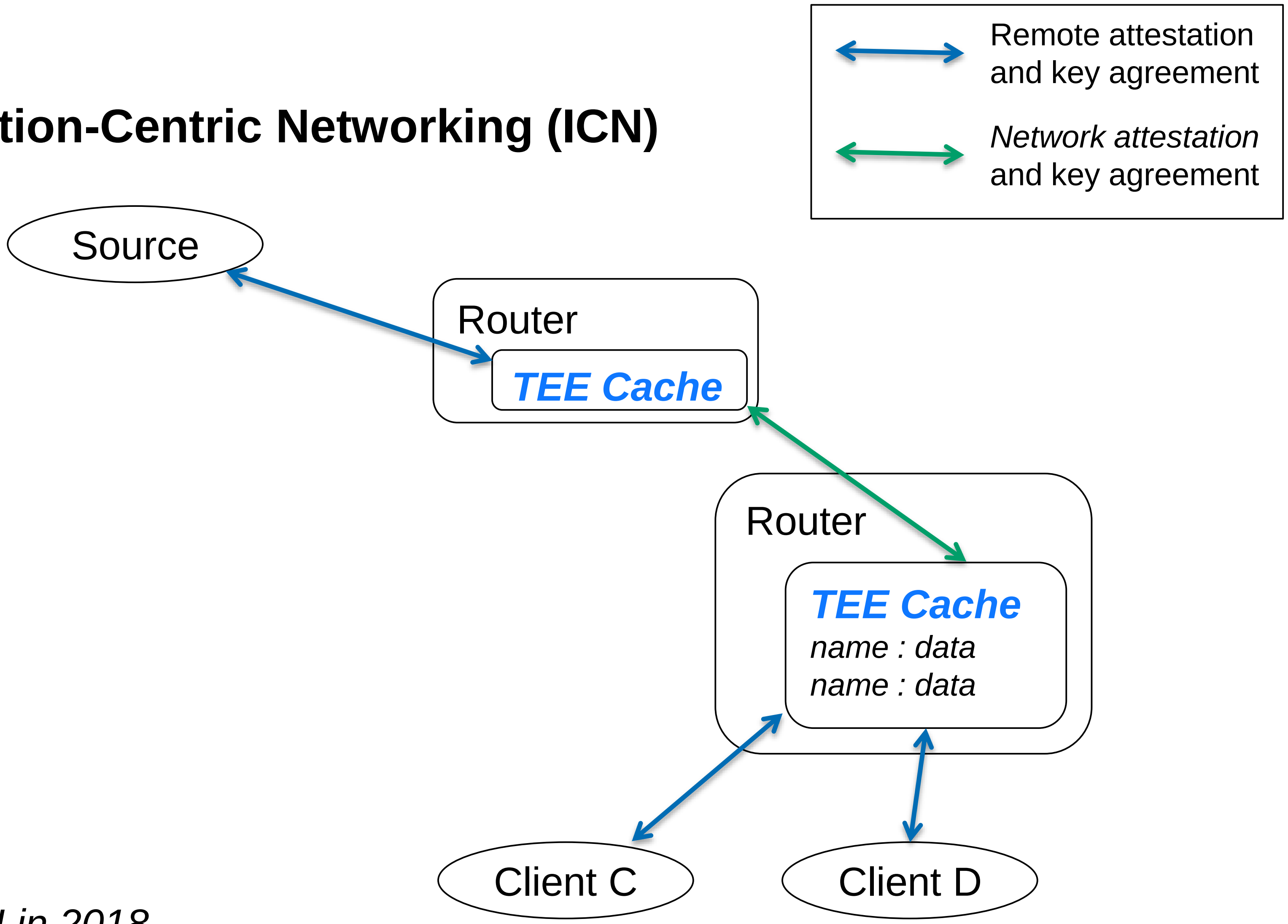
New Communication Paradigms (1)

Security and privacy in **Information-Centric Networking (ICN)**



New Communication Paradigms (1)

Security and privacy in **Information-Centric Networking (ICN)**



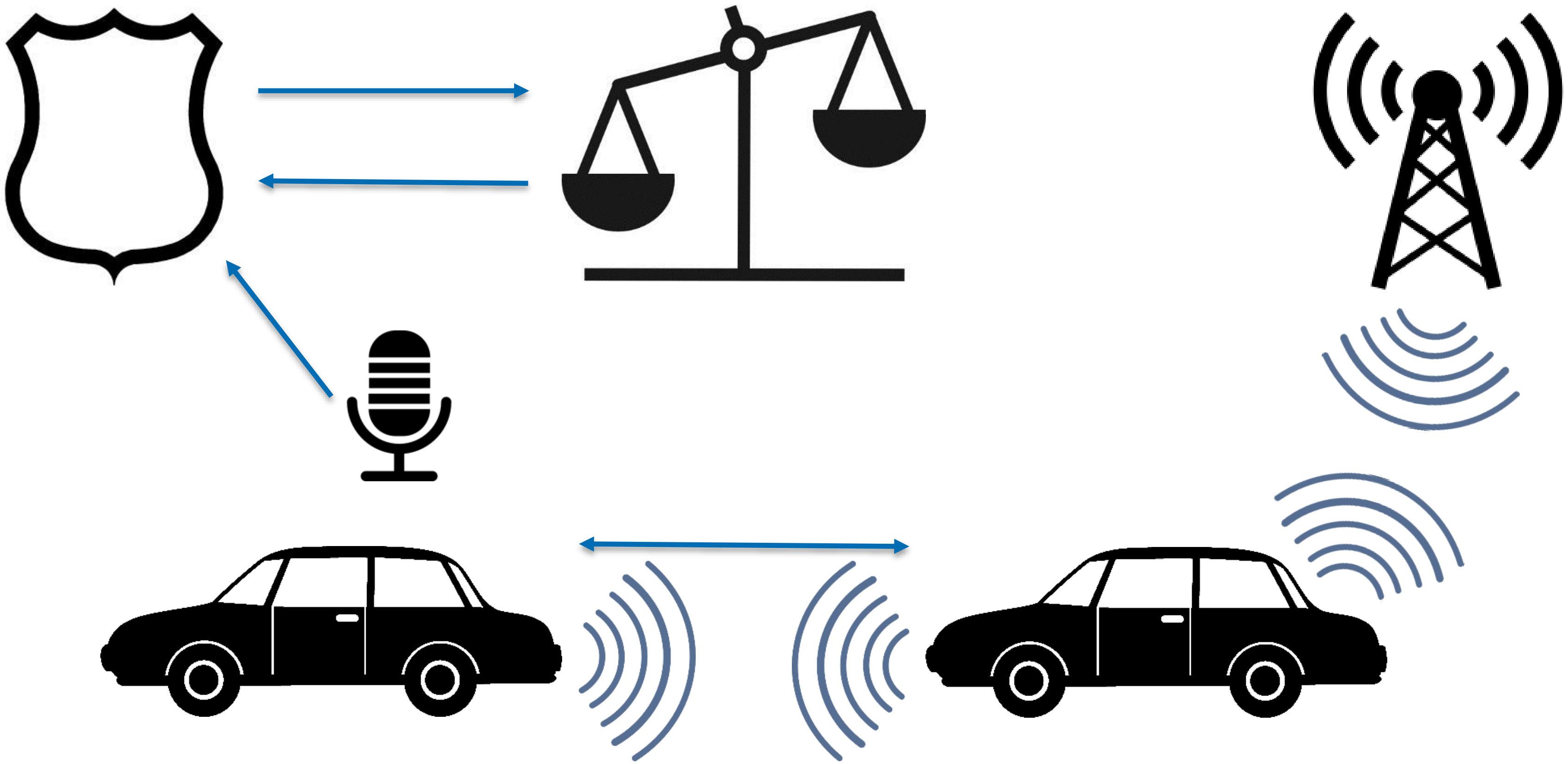
Research challenges

1. Define appropriate security and privacy guarantees:
   - Request privacy
   - Data privacy
   - Cache privacy
2. Protocol design and analysis
3. Performant implementation

FULBRIGHT COMMISSION *Research visit to UCI in 2018 (Fulbright Cyber Security award)*

New Communication Paradigms (2)

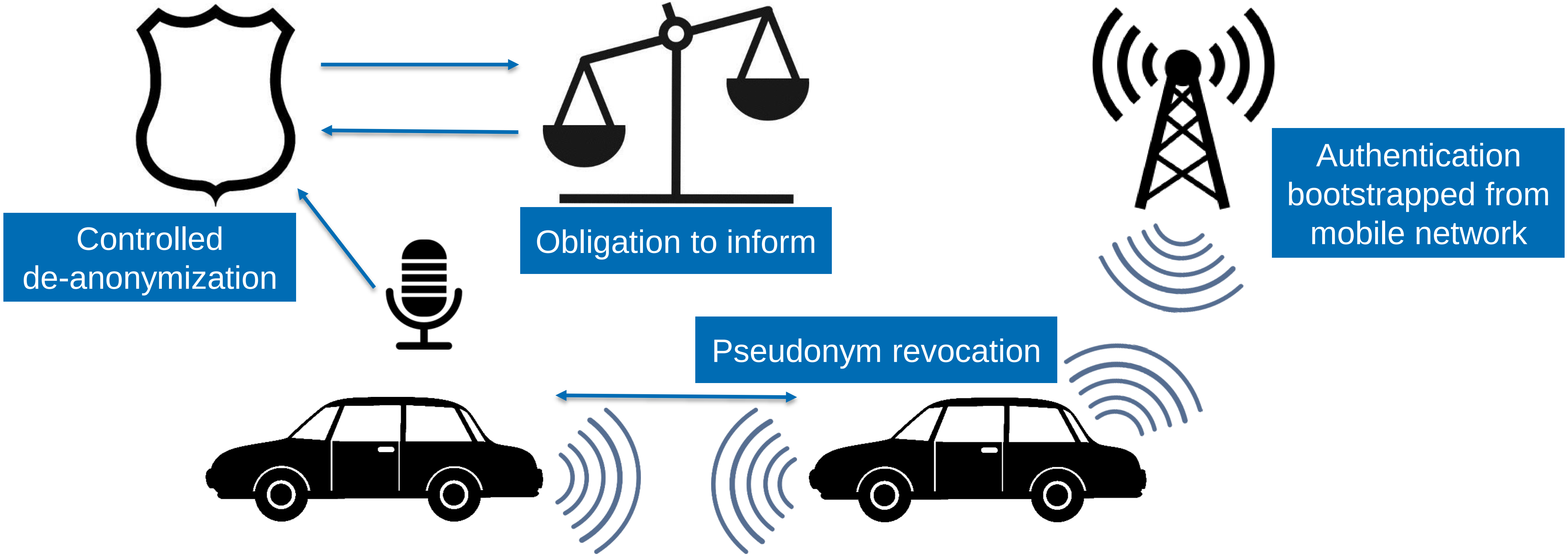
Vehicle-to-X communication



New Communication Paradigms (2)

Continued collaboration with Whitefield, Chen, Schneider, Treharne

Security and privacy in **Vehicle-to-X communication**



Art 33. Obligation d’informer les personnes surveillées
https://www.admin.ch/opc/fr/federal-gazette/2015/6597.pdf

Research commenced at Aalto as part of V2X and 5G project, funded by Intel.

Improving Energy Efficiency

Energy-efficient distributed consensus

Existing work

- Maximizes transactions per second

Aim

- Maximize transactions per joule

Approach

- Reduce number of messages using trusted execution environments and remote attestation

Research challenges

- Protocol design and analysis
- TEE implementation
- Quantify energy-efficiency improvement

Use cases

- Autonomous embedded devices

J. Liu, W. Li, G. Karame, N. Asokan, [Scalable Byzantine Consensus via Hardware-assisted Secret Sharing](), arXiv:1612.04997 [cs.CR], 2017.

Research commenced at Aalto in collaboration with NEC Labs Europe.

Support Full System Life-Cycle

1. Device manufacture
- Key/pseudonym provisioning
- Attested supply-chain security

2. Remote configuration & updates
- Configuration privacy
- Personalized updates

3. Ownership change
- Key/pseudonym rotation
- Attested data protection

4. End-of-life
- Key/pseudonym revocation
- Attested data deletion

Research commenced at Aalto as part of SELIOT project with UCI and UF.

Proposed research

Use trusted hardware and remote attestation across the full spectrum of systems to:

1. **Enable new communication paradigms**
   - e.g. information-centric networking, ad-hoc networks (V2X)

2. **Improve energy efficiency**
   - e.g. energy-efficient distributed consensus

3. **Support the full system life-cycle**
   - e.g. provisioning, ownership-change, and revocation of IoT devices

Supported by: **formal protocol analysis, collaboration with domain experts, collaboration with other disciplines (e.g. law).**

Andrew Paverd

andrew.paverd@ieee.org