Authenticating Pervasive Devices with Human Protocols

Ari Juels
RSA Laboratories

Stephen A. Weis
MIT CSAIL

Pervasive Devices

- Pervasive Devices:
  - Low memory, few gates
  - Low power, no clock, little state
  - Low computational power
- Billions of pervasive devices are deployed.
- Billions on the way.

Can such feeble devices authenticate themselves?

Example Technologies

“Billions and Billions...”

- Supply chain management, inventory control
- Payment systems, building access
- Prescription drug shipments
- Retail checkout
- Luxury goods
- Currency

Authenticating devices is a growing concern.

Attacks

- **Skimming**: Reading legitimate tag data to produce fraudulent clones.

- **Swapping**: Steal RFID-tagged products then replace with counterfeit-tagged decoys.

- **Denial of Service**: Seeding a system with fake, but authentic acting tags.

Related Work

- Low-Cost Access Control:

  [SWE02], [WSRE03], [OSK04]

- Pervasive Privacy:

  [JP03], [JRS03], [Avoine04], [MW04]

- Human Authentication: *[HB01]*

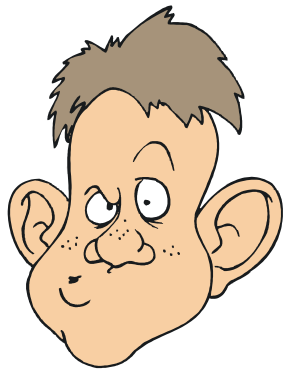
Our Contribution

- A new authentication protocol that handles active malicious attacks.
- Extremely hardware-efficient
- Secure under same assumption as [HB01]

Hopper-Blum Authentication

Computer(**x**)

Bob(**x**, η)



$\mathbf{a} \in \{0,1\}^k$

Challenge

$z=(\mathbf{a}\cdot\mathbf{x})\oplus\nu$

$z=(\mathbf{a}\cdot\mathbf{x})$?

$\nu \in_R \{0,1\}$

Response

Repeat for q rounds.

Authenticate Bob if he passes > (1- η)q rounds.

Security Against Bad Bob

Computer(**x**)

$\mathbf{a} \in \{0,1\}^k$

Challenge

$z=(\mathbf{a} \cdot \mathbf{?})$

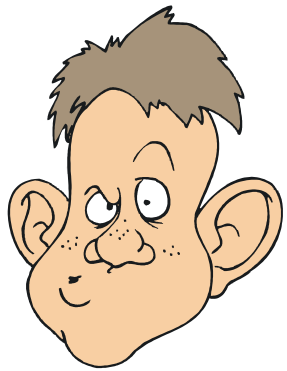
Guess Response

Adversary

Security Against Passive Eavesdroppers

Computer(**x**)

Bob(**x**, η)



$\nu \in_R \{0,1\}$

Eavesdropper

$(\mathbf{a_0}, z_0), (\mathbf{a_1}, z_1), \ldots, (\mathbf{a_q}, z_q)$

Find an **x'** that allows you to answer a (1- η) fraction of **a** challenges

Learning Parity with Noise (LPN)

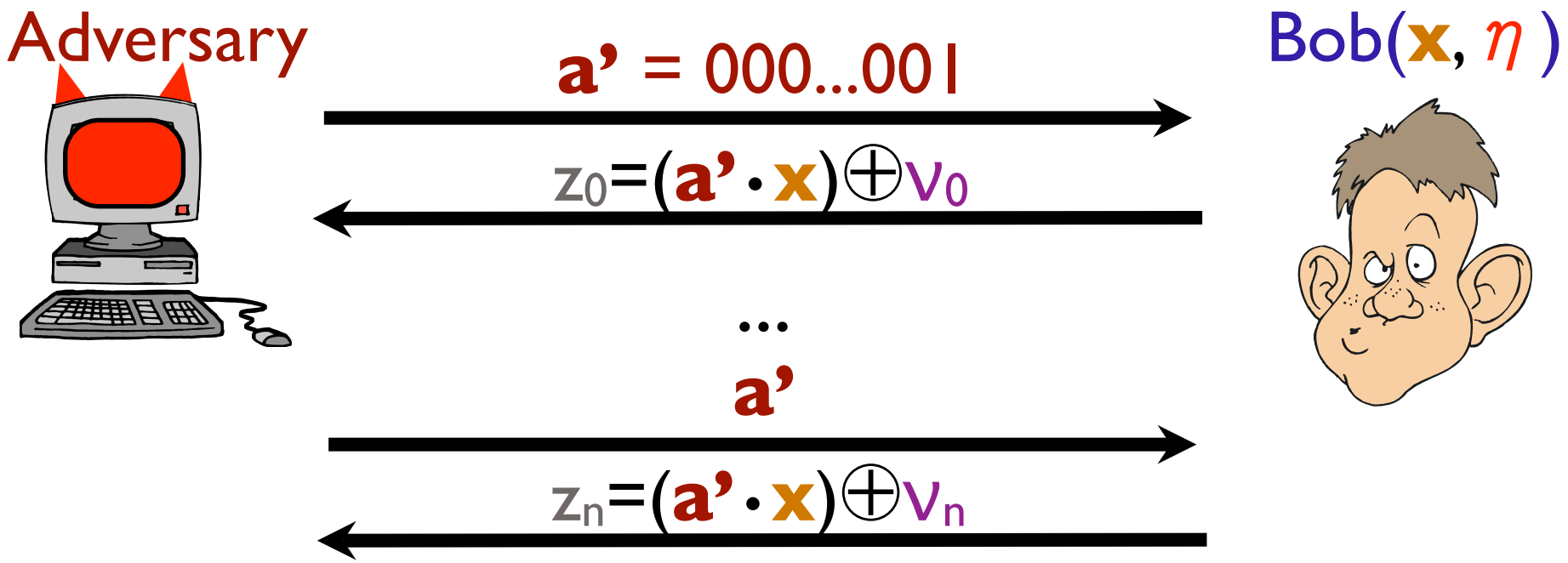
- Crypto and learning problems: [BFKL93]
- $O\left(2^{\frac{k}{\lg k}}\right)$ LPN algorithm: [BKW03]
- Shortest Vector Problem reduction: [Regev05]

Concrete Security

Key Size (k)	Best Attack
64	2^{35}
128	2^{56}
192	2^{72}
224	2^{80}
256	2^{88}
288	2^{96}

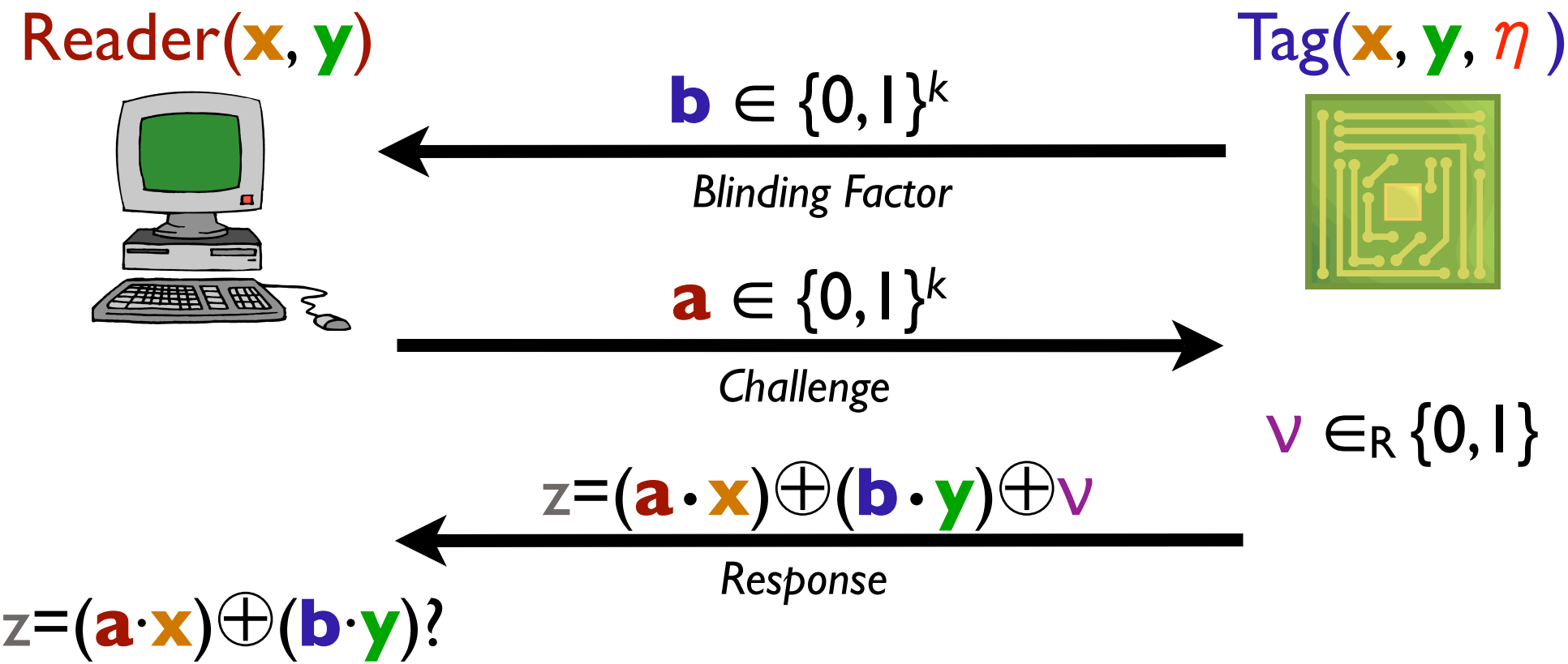
Obligatory grain of salt →□

Active Attack against HB

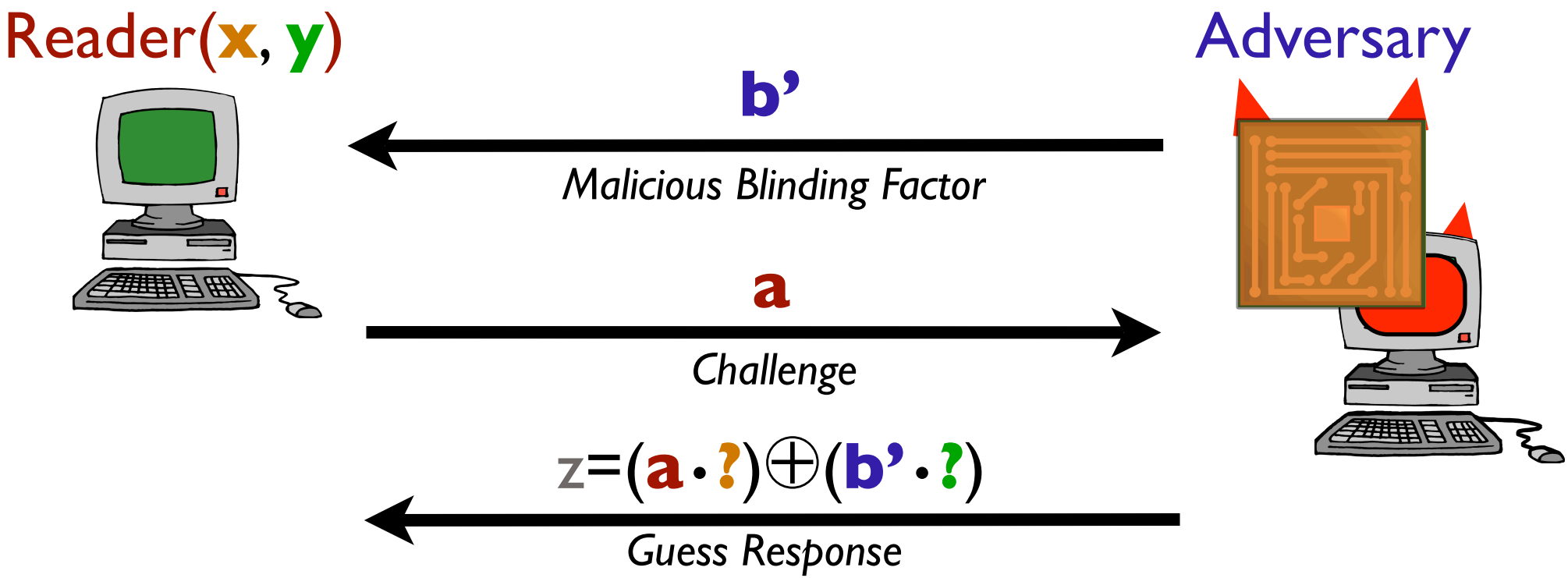


Adversary takes majority of z_i values to get noise-free parity bit

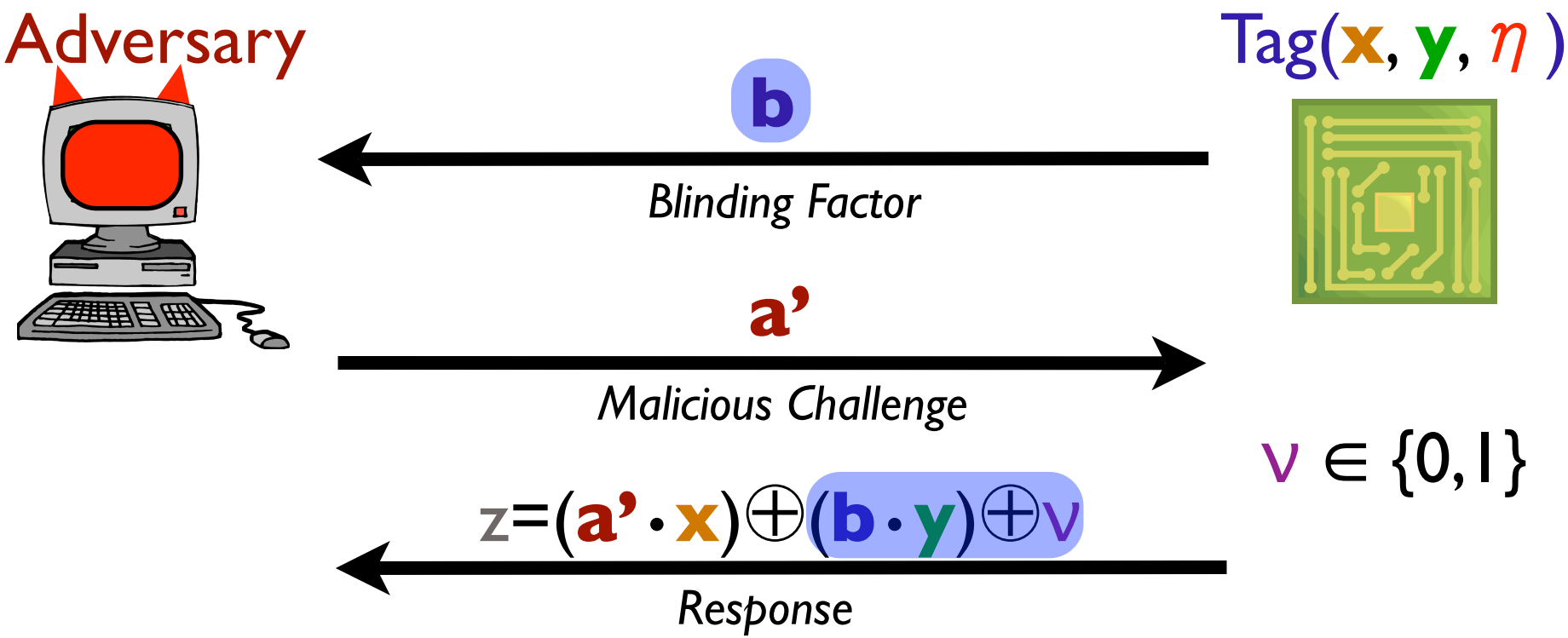
Our New Protocol: HB+



Security Against Bad Bob



Security against Active Attacks



Skewing Randomness

What if the adversary can skew a tag's random number generator?

All bets are off!

Future Work

- Two-round or ~~parallel~~ HB+ *(Rump Session)*
- Random Number Generation
- Underlying hardness of LPN
- Adapting other HumanAuth protocols

Questions?

Ari Juels

ajuels@rsasecurity.com

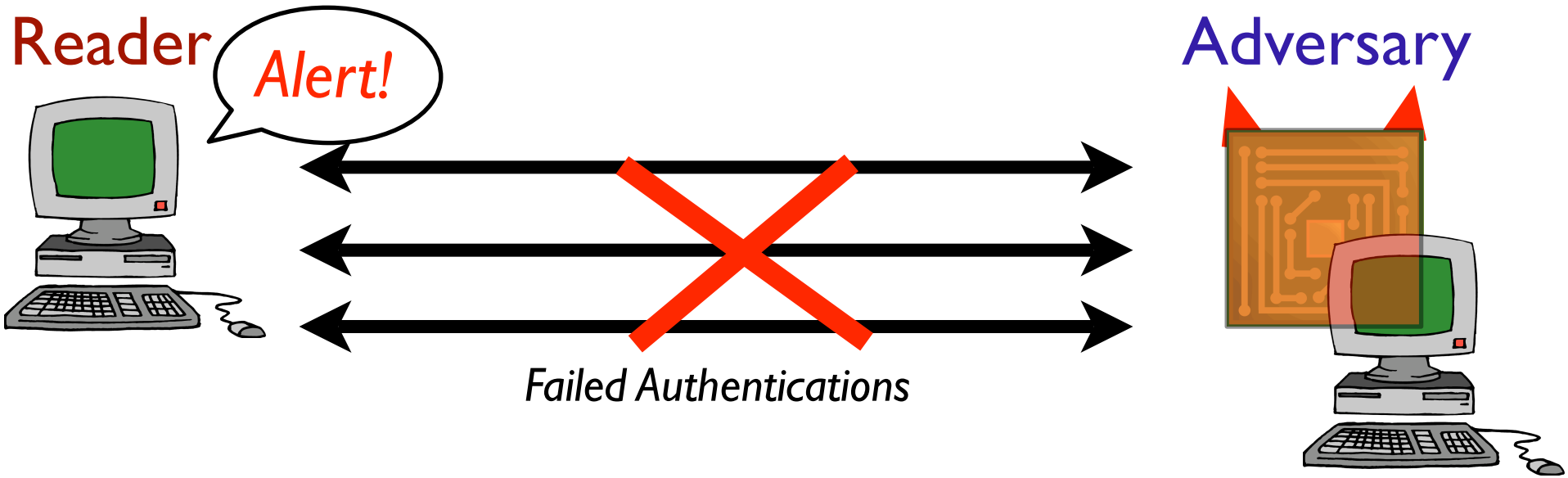
www.ari-juels.com

Stephen Weis

sweis@mit.edu

crypto.csail.mit.edu/~sweis

Detection Security Model



Assume valid readers will detect suspicious failures:
No Reader oracles.