The Drawbridge Model of Cryptographic Communication:

A Framework for Sociocultural Analysis of Information Security

Charles Berret

Linköping University

WASP-HS Cybersecurity
26 March 2024

A Situated, Sociocultural Approach to Crypto

What can we learn about concealing communications by studying different forms of communication failure?

A Broad Definition of Cryptography: Any form of communication that uses known sources of communication failure to create reversible, nondestructive encodings that selectively limit the audience of a message.

Cryptography as Drawbridge: Information security techniques work by selectively raising and lowering the drawbridge of communication's success or failure.

Drawbridge Model of Cryptographic Communication

- Chain of islands separated by gaps. Each gap is a potential source of communication failure.
- Successful communication must bridge each gap. Failure at any stage makes further stages inaccessible.
- Different information security techniques cause communication failure at different stages. This failure must be *selective* and *reversible* (like a drawbridge).

Access

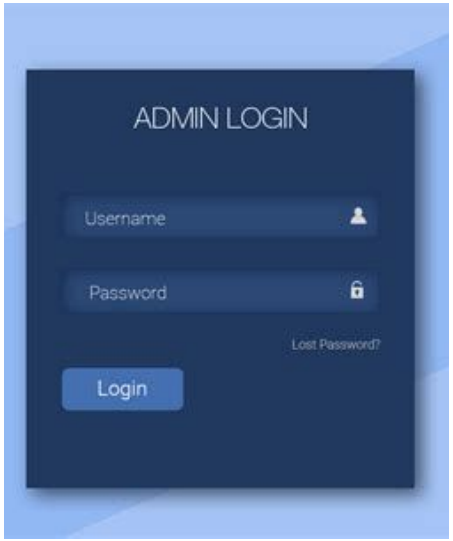
Definition

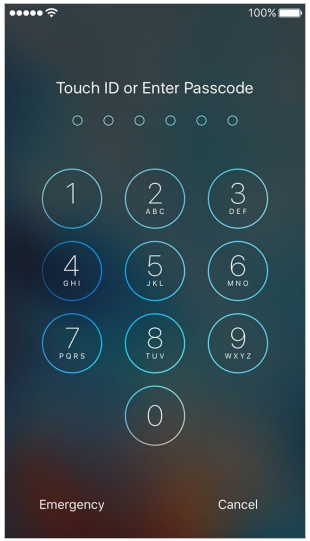
- Barrier or lack of authorization keeps you from receiving a message.
- If message is inaccessible, comm fails even if message is perfectly viable otherwise.

In Practice

- *Mundane Failure*: Barriers, Lockouts, Forgotten Passwords.
- *Security Schemes*: Keys, Envelopes, Logins, File Permissions.

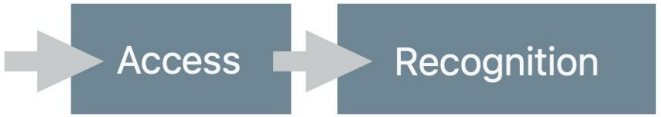
Access-Based Security





	View	Edit	Create	Delete
User	☑	☑	☑	☑
Class			☑	
Class Manager	☑			
Role	☑	☑	☑	☑
System Status	☑			
System Settings	☑	☑		
Custom User Fields	☑	☑		
Active Users	☑	☑		

Recognition



Definition

- Given Access, Recognition is the awareness that a specific message or information is present.
- Communication fails when we do not recognize that the message is there.
- The message could be perfectly viable otherwise, but communication still fails if unrecognized.

In Practice

- *Mundane Recognition Failure*: To wave, but someone doesn't see; to overlook information buried in a footnote.
- *Security Schemes*: Steganography, Invisible Ink, Digital Watermarks.

Recognition-Based Security

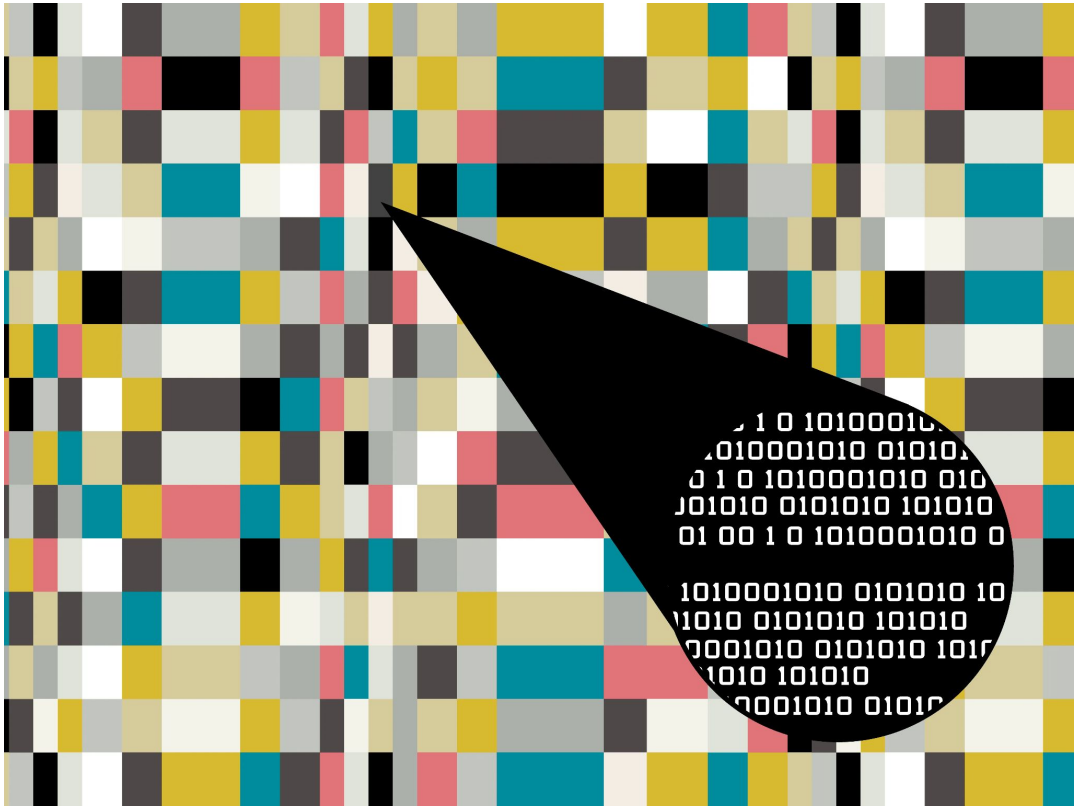


Image: Wired.

Legibility

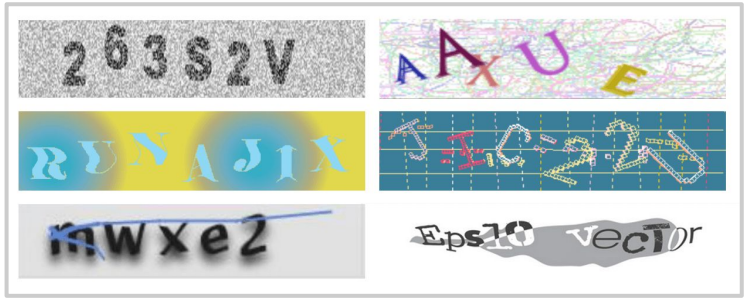
Definition

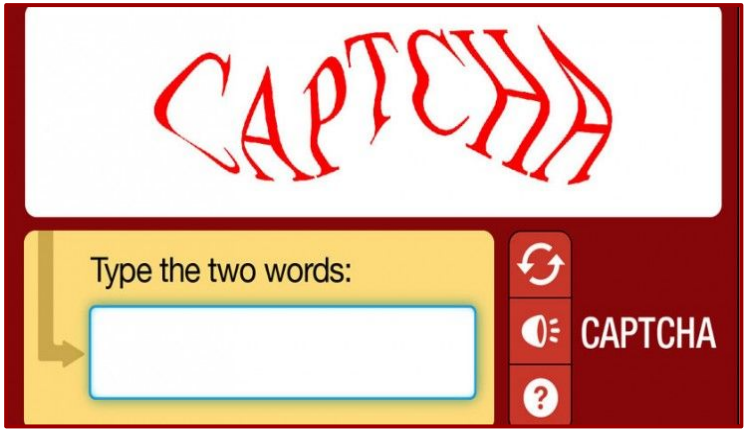
- Specific definition for this model: a *legible* message is rendered in symbols known to the user.
- “H” vs. “□”

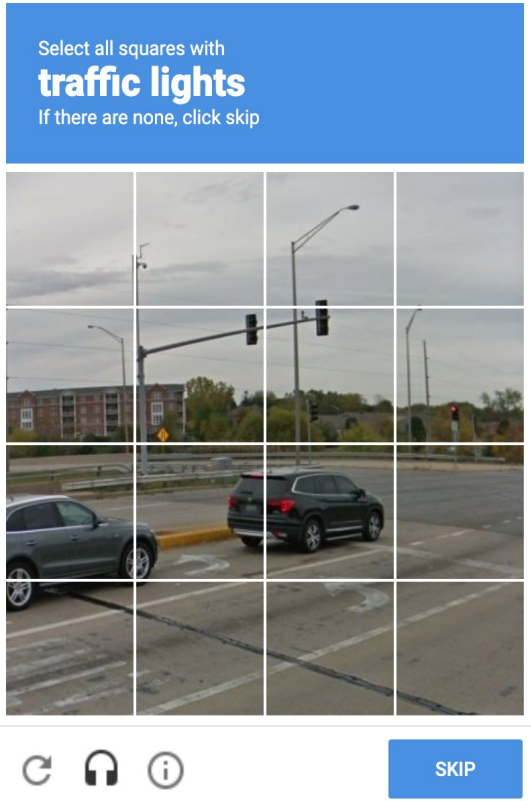
In Practice

- *Mundane Legibility Failure*: optometry exam, illegible handwriting, undeciphered ancient scripts (e.g. Linear A)
- *Security Schemes*: CAPTCHA.

Legibility-Based Security



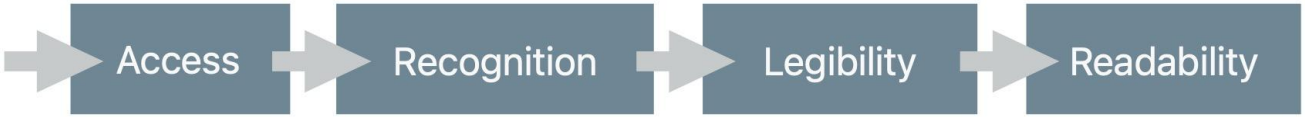




Legibility-Based Security

ZXX typefaces by Sang Mun (2013)

Readability



Definition

- Ability to recognize coherent patterns, words, syntax, in a set of known symbols.
- “HELLO” plaintext / “YDVQP” ciphertext.

In Practice

- *Types of Mundane Failure*: spelling and encoding errors, incompatible file formats, bit rot.
- *Security Schemes*: anagrams, acrostics, digital encryption of messages.

```
hQIMAw3Jn/nLK/38ARAAsSXLDhCtzUYKMptNxZImJXwhhIRm3QxfuyHjJ93ASylE
e+6ABkuyFLJhiKryxp/JmS/alMPfF7hx2aTgovagaPzTwTV1jo6If2mhdCl6keed
1Iz7C0f6jHIqq9d8g0bWDyvELEipn5LNDTX3Xp2Csx5ojRB2wckrUt1l1Xyj8G0H
4DQUYbINRmJVulJJC/acGvgOze66pHuRgSCxxHDscefjXenh/XejSYTo7aMi+Es7
DCcD49zH6ZLDQN6BlN9q2oFI8QIhQ2y1QJbat1dWi/4yYWlKZcLKRSm8eo/gNCdL
h9MncXBBSfgbvbu67CDZ9GO5geZOn3LzQOpJ8hrZq/6K/uMcUKeZjW3RCo0T754f
E5zYe1wUgtwS/lmQ2w5PQF/89bpshtDSYuL1fZgzrsE6DwophuCri5zwCGbEKlsI
g6REIETFbZ2aCL4N2pZVunCIEuoP0zgEB6+M9egdpyxMsMqEBVg3AH7Sa1AtEguP
T/MCxI0bZHCUhPupEKT8slbSrDNxTWMUXQt3XpL0bGCCrDMKLSoWYfDiNnRkFbWK
iiqw9hx4Q9CJg7xX7JRnVgwOeREiFnMYSbFlvPSxEOu6FdBYhdqSefKin4Wnkmdw
qrSl8fjIW/kZ2v72uz0buEKkY9ubBox76yjlRo9KUQMs3em03kc64959gTDiZ0qF
AgwDrosDPQ2BeYQBD/9H5VKFw0an5j5MX1JpOSBAqNGKWq2bcEFnwJfk0DDlhyHD
owHiG7gDowCS+5y/pf56v36HkzpJZATKqoRyKVxmQOxU9l3YnPc5fw8iFhxlrfcG
ywzkJh/BRDQ/uy5fhGc/PbSm6iLv/SkkWTK8PSUD+g1yZyK0W7WkMh9QYS2OE7lQ
qbwpNiy57reWkUWCoE4QmKqqpe7NXXM0eLT9l2D0hG2lthyvTvspkpxszl8+HMJv
M2LMcY2FmmZWAJSdxsQSq9NQdyvCJX2D8oa89WQyXmp7mPXL7BQfoQNPndmn6Obi
0EQojoeMRNh14XNhMjPjxW7m34rH2gtvdN3Dg8iFrtocoVJqXqU3N+9T2sNe/bS8
```

Meaning

Definition

- *Success*: Shared intersubjective accord on the content expressed in a message.
- *Failure*: Mistaken apprehension, confusion, apparent nonsense.
- *Selective Mediation*: Assignment of new meaning to a specific message (Social Steganography, Marwick & Boyd).

In Practice

- *Types of Mundane Failure*: Deception, misunderstanding, false attribution.
- *Cybersecurity Threats*: Spoofing, phishing.

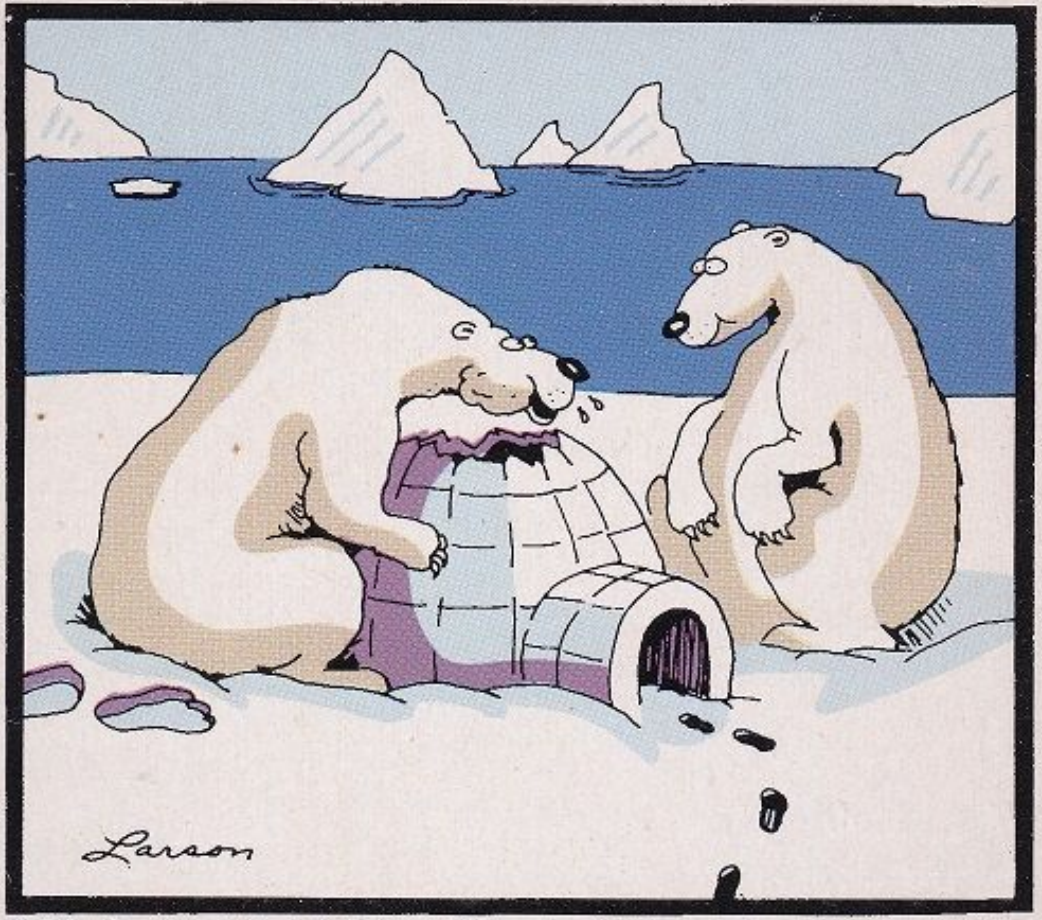
Meaning-Based Security Threats

Image: Security Magazine.

Drawbridge Model of Cryptographic Communication

Implications for AI and Cybersecurity

- Different forms of information security leverage different kinds of communication failure to selectively divide the audience of information.
- Modeling threats and vulnerabilities using the Drawbridge Model can help develop defense in depth by evaluating strength of security at each stage.
- Identifying the ways AI succeeds and fails at communication can point to opportunities for building better defenses.



"Oh hey! I just love these things! . . . Crunchy on the outside and a chewy center!"

Thank you!

charles.berret@liu.se

https://charlesberret.net

The Drawbridge Model of Cryptographic Communication:
A Framework for Sociocultural Analysis of Information Security

Charles Berret

WASP-HS Cybersecurity
26 March 2024