Trustable Internet Research Concept

J. Mark Pullen

George Mason University C4I & Cyber Center

PROBLEM

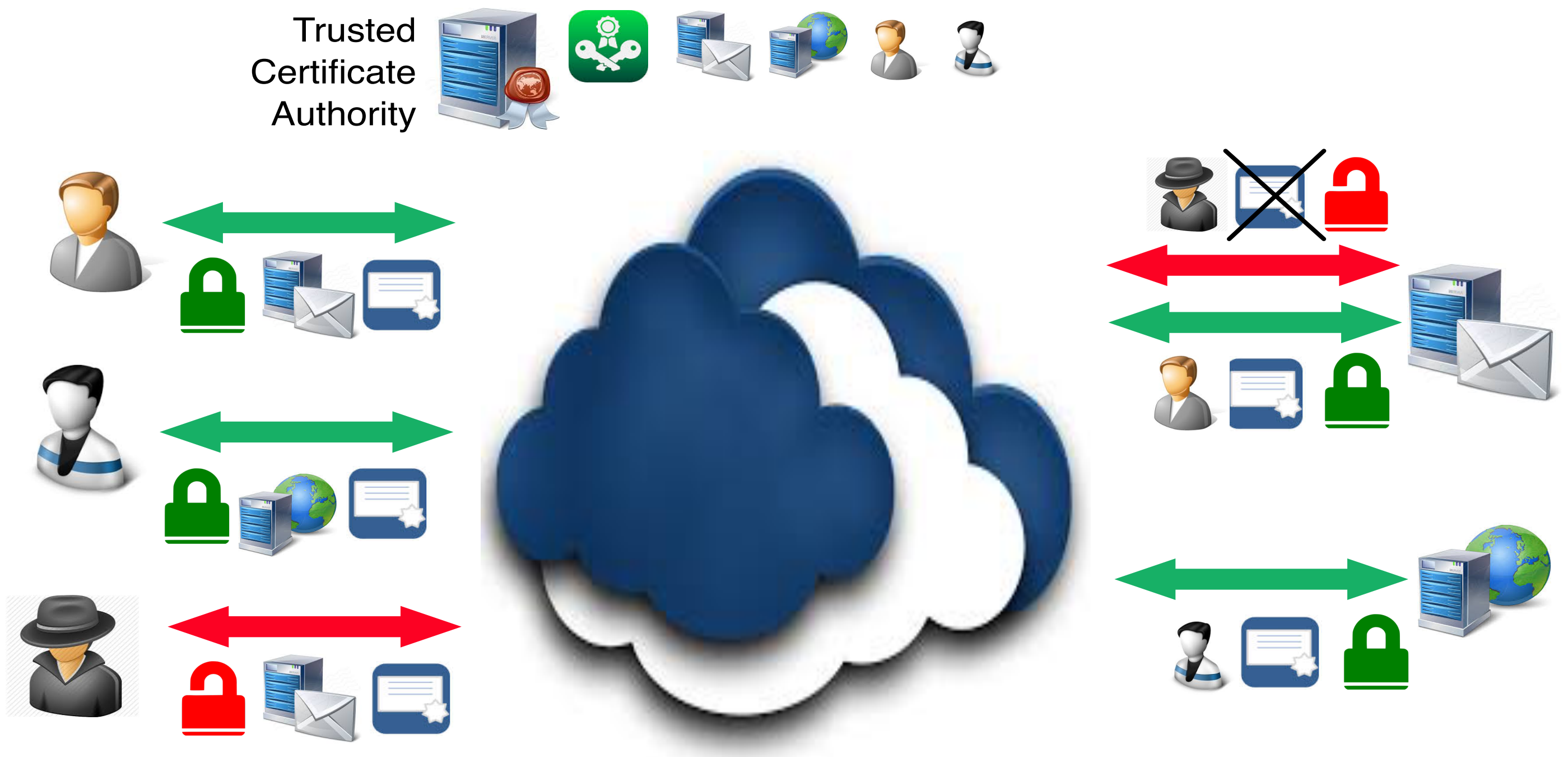
- **The Internet has a fatal flaw**. The flaw is not in the Internet itself, but in how the connected computers use it. They do not insist that every connection be verified trustable.
- The computer should be built so it will not make a connection before using Internet protocols to establish trust.
- Implementing mechanisms for two way trust will not come easy as it requires processes for identity verification and the loss of anonymity. Some users love anonymity but it is the root of many problems.
- **Forced trust verification will eliminate a range of malicious attacks and provide traceability for those that are not eliminated.**

INTERNET SECURITY SOFTWARE

- The Internet Protocol Suite already includes all the features necessary to establish and verify trust, but they are not used by most applications. These include:
  - Public key infrastructure (PKI) that provides a trustable, easy to use way to get encryption keys.
  - Reliable, effective encryption implementations that use these keys to ensure a third party can't eavesdrop or connect without a key that is considered trusted.
  - That's all we need from the Internet!
- But today's Internet was deployed without mandating these features, because processors of the time could not cope with the computation demands of security.
- In place of trust a large number of "band-aid fix" programs has been developed. They do not get at the fundamental problem – as long as untrusted connections are allowed our computers will remain vulnerable to ever-increasing exploits.

EXISTING APPROACHES

- **Existing browser technologies are already moving towards forcing websites to use encrypted HTTPS connections**.
- The "HTTPS Everywhere" project by the Electronic Frontier Foundation and the Tor Project provides browser extensions that force secure connections where available. However, their focus is on confidentiality and not two way trust verification.
- The mechanism behind HTTPS, Transport Layer Security (TLS), provides for two way verification of both communication end points, but is not widely used outside of corporate and government environments because of a lack of infrastructure and easy to use verification tools.



OUR APPROACH

- **We need a modified end computer that will never make a connection without established trust. This should be mandated at the operating system level.**
- And an easy-to-use interface to designate trusted others.
- And a campaign to get the world to use this: policy and education.
- The result will be an Internet with two disjoint user communities that cannot communicate with each other.
- The trusted community will be free of malicious attacks except where a user is gulled into a poor choice of trusted partner.
- And even there the source will be traceable. No more spam!

FUTURE URGENCY

- **In 2016, there will be 6.4 billion Internet connected devices.**
- **That total is predicted to reach some 20 billion connected consumer, business, and industrial devices by 2020. [2]**
- These devices will be constantly communicating not just with humans, but autonomously with each other and to Internet cloud based services. Their functions will be critical to human health and safety.
- Securing these devices and managing their interactions has security implications in protecting the privacy and verifiable trust of the data that they generate and monitor.
- New approaches are required to allow for distributed and decentralized trust verification.

RESEARCH AREAS

- PKI implementations that can be made widely available freely or at little cost and include identify verification for client side authentication
- Distributed trust verification using blockchain technologies
- Operating System mechanisms to force two level transport layer security verification for all connections
- Policy requirements to socialize and support implementation
- Determining an effective educational program to inform users