CryptoRave 2014

Quais são os limites das tecnologias atuais para combater a vigilância em massa? Quais são os novos projetos e as soluções que estão sendo desenvolvidas?

Breve em https://rhatto.sarava.org/cryptorave

CRIPTOGRAFIA FUNCIONA: AS SOLUÇÕES E OS LIMITES ATUAIS

"Communicação nerd a nerd está OK, mas e quanto ao mundo real? E quanto aos meus amigos/as? E quanto à minha família?"

-- Dan Kaminsky, pesquisador de segurança.
http://mashable.com/2013/03/04/wickr/

TL;DR

1. Neutralidade: a rede deve ser apenas o entregador das mensagens, lidando apenas com endereçamento.
2. Endereçamento seguro: criptografia ponta-a-ponta de dados e metadados.
3. Sistemas e protocolos estão em disputa pela padronização.
4. É mais fácil resolver a etapa da rede do que a segurança nos dispositivos dos usuários.

Software livre: é pressuposto!

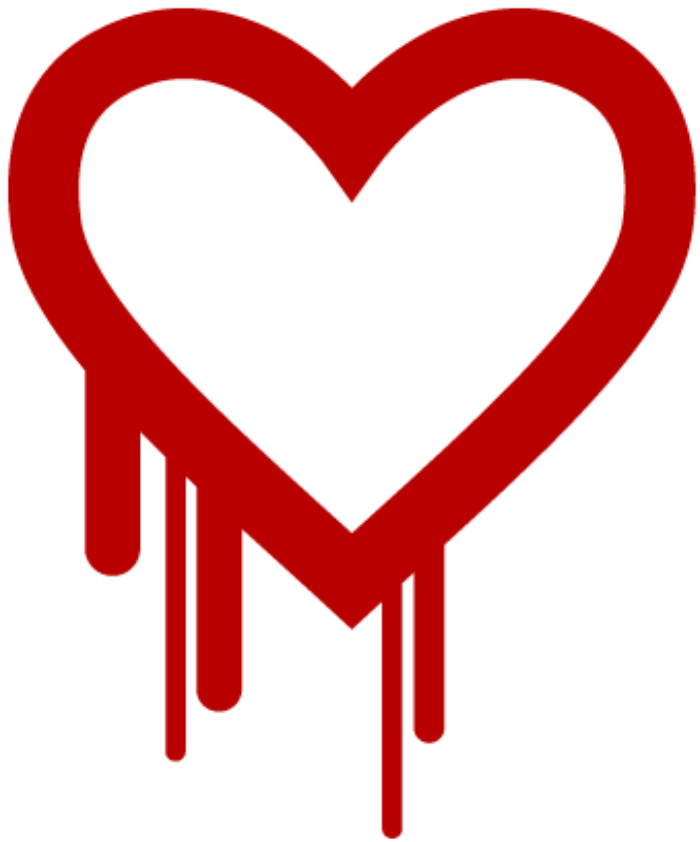
O sexteto da segurança:

- As quatro liberdades: rodar, estudar, redistribuir e melhorar programas.
- Princípio de Kerckhoffs: o sistema deve ser seguro mesmo se tudo do sistema é conhecido, exceto as chaves.
- Lei de Linus: quanto mais olhos no código, mais bugs são encontrados.

Consideramos que os sistemas são conhecidos. Mais ainda, devemos torná-los conhecidos para que possam ser melhorados!

Software livre: não é condição suficiente para segurança!

- O que um olho não viu pode existir!
- O que um olho viu e não publicizou pode ser explorado maliciosamente!
- Software desatualizado é parque de diversões alheias.
- Com software proprietário o problema é muito pior!



Segurança na rede

- Para que mais olhos enxerguem, precisamos de soluções com massa crítica.
- Que operem fora de silos e jardins murados.
- Fator Babel: de tal modo que que se tornem **padrões** e **ubíquas**
- O comportamento seguro deve ser o *padrão*

A pergunta central é: para mudarmos os protocolos, a melhor estratégia é:

1. De ruptura: criamos novos serviços seguros e encorajamos a migração direta dos/as usuários?
2. Incremental: upgrade transparente de protocolos conforme os softwares forem atualizados?

Os grandes problemas

- Há uma série de problemas difíceis de serem resolvidos, especialmente porque para eles não existe consenso ou mesmo propostas de soluções.
- Assim, a estratégia será incremental!
- Ei-los: gestão de chaves, proteção de metadados, assincronicidade com sigilo futuro, comunicação em grupo, compartilhamento de recursos, disponibilidade, atualização e autenticação seguras, facilidade de uso, etc.

https://oblivia.vc/pt-br/content/problemas-difíceis-na-comunicação-segura

Aprendendo com os erros...

- Exemplo limite: Lavabit: qualquer nova plataforma deve ter um modelo de ameaças mais resistente.
- Exemplo ruim: Telegram: não crie protocolos em casa e forneça-os como serviço de massa sem antes submetê-los ao escrutínio público.

Comparativo entre arquiteturas

	Peer to Peer Encrypted	**Silo** Encrypted	**Federated** Encrypted
Availability	Lower	Higher	Lower
Usability	Lower	Higher	Lower
Compatibility	Lower	Lower	Higher
Authenticity	Higher	Lower	Higher
Control	Higher	Lower	Higher
Anonymity	Higher	Lower	Lower

Relatively better is not necessarily good. For example, federated and peer-to-peer models have better authenticity than silo models, but still in practice have many authenticity problems.

Figure: https://leap.se/en/docs/tech/infosec

LEAP Encryption Access Project

- Foco: autenticidade, usabilidade e proteção de metadados.
- Serviços: email, VPN, mensageria.
- Plataforma automatizada no lado do servidor.

		Federated Cleartext	**Federated** Encrypted	**LEAP** Encrypted
Message Security	Confidentiality	None	High	High
	Integrity	None	High	High
	Availability	Medium	Medium	Medium
Identity Security	Authenticity	None	Low	**High**
	Anonymity	None	Low	Low
	Unmappability	None	None	**High**
User Freedom	Control	Medium	Medium	Medium
	Compatibility	High	Medium	**Low**
	Usability	Medium	Low	**High**

Figure: https://leap.se/en/docs/tech/infosec

Outras plataformas

- Relatório sobre projetos de comunicação segura: https://github.com/OpenTechFund/secure-email
- TextSecure: abre perspectivas para mensageria instantânea.
- DarkMail, SilentCircle, Wickr, etc: abrirão o código?
- Sistemas de cauda longa (Pond, Enigmabox, etc): https://rhatto.sarava.org/services/
- Voz e vídeo (ZRTP).

Segurança dos dispositivos

- Sistemas operacionais mais seguros.
- Hardware aberto: evitando backdoors.
- Geração satisfatória de números aleatórios.
- Agoritmos e protocolos criptográficos do estado da arte.
- Armazenamento criptografado.

Segurança mental

- Como resolver o problema das senhas?
- Fácil de lembrar, fácil de quebrar.
- Gerenciadores de senhas.
- Biometria: facilmente forjável.
- Tokens afanáveis?
- Implante de senhas e chaves? :P

Perspectivas e previsões

Poderíamos pensar numa agenda cypherpunk para segurança de massas?

Criptografia

- Difícil de prever, depente de descobertas paradigmáticas!
- Aplicação do estado da arte na prática: computação homomórfica, zero-knowledge!

Hardware

- Onde estão as foundries locais?
- Será mais fácil produzir plataformas abertas?
- Patentes e propriedade intelectual afeta especialmente o hardware.

Softwares

- Linguagens de programação e frameworks pró-ativos.
- Bibliotecas com melhores implementações de primitivas criptográficas (NaCl, cripto++, RELIC, polarssl, GnuTLS...)
- Checagem a integridade de código fonte e binários deve ser a regra (assinaturas, compilação determinística).

Protocolos e Serviços

- Superar problemas difíceis.
- Disputar com protocolos e serviços menos seguros.
- Conseguir o apoio da base de usuários/as.

Financiamento

- Desenvolvimento em seguraça custa caro pois demanda estudo e cuidado!
- Crowdsourcing e micropagamentos.
- Modelos de negócios diretos ao invés da espionagem e mineração de dados, com serviços massivos a preços acessíveis.
- Que permita auditoria dos softwares, plataformas e serviços.

Educação

- Maior acesso ao público de informações sobre segurança.
- É preciso incentivar uma nova geração de estudantes de criptografia! :)

Legislação

- Marcos regulatórios compatíveis com requisitos de privacidade (sem retenção de dados, por exemplo).
- Mesmo num cenário draconiano a tecnologia consegue evadir medidas de vigilância.

Fim

- Perguntas?
- Podemos fazer previsões para os próximos cinco e dez anos?
- rhatto @ sarava.org / https://seguranca.sarava.org / https://oblivia.vc
- OpenPGP 66CA 01CE 2BF2 C9B7 E8D6 4E34 0546 8239 64E3 9FCA