OP3FT

FROGANS TECHNOLOGY

ICANN58 – Copenhagen
Emerging Identifiers Technology Panel Session

Frogans addresses: a new security model for a new type of online publishing built on top of DNS

Alexis TAMAS, co-creator of Frogans technology
alexis.tamas@op3ft.org

March 14, 2017

Introduction (1/5)

- Frogans technology is a secure technology for the publishing of content on the Internet
- It enables the implementation of a new software layer on the Internet, called the Frogans layer, alongside other existing software layers such as E-mail or the Web
- Frogans technology introduces:
  - a new type of online content, called Frogans sites
  - new software to navigate Frogans sites, called Frogans Player
  - new Internet identifiers for Frogans sites, called Frogans addresses

Introduction (2/5)

- Frogans addresses were designed with the following original goals:
  - they had to be short and simple
  - they could not contain any technical information
  - they had to clearly stand out in various contexts
  - they had to be original so that users could easily distinguish them from other Internet addresses

Introduction (3/5)

- URIs and domain names were not chosen as a basis for Frogans addresses as they could not directly achieve these original goals without modifying their scheme or syntax
- The DNS technically could not be used to resolve Frogans addresses: the size of the data resolved for a Frogans address was expected to be too large (between 1,900 and 4,800 bytes) and that size could increase in the future
- However, the Frogans layer requires DNS to function in order to address the servers used to:
  - resolve Frogans addresses (.frogans TLD)
  - host Frogans sites (any gTLD or ccTLD)

Introduction (4/5)

- Furthermore, OP3FT, the non-profit organization which holds, promotes, protects and ensures the progress of Frogans technology, applied to operate the .frogans TLD
- The objective of .frogans is to ensure the security, stability and reliability of the Frogans layer for the benefit of all Internet users
- The .frogans TLD domain names are only used to address the computers dedicated to the functioning and administration of the Frogans layer on the Internet
- The key benefit in using a TLD instead of a second-level domain is to gain maximum control over the registration process and resolution of these critical domain names

Introduction (5/5)

- Frogans addresses enable a new security model for online publishing, which is based on a cohesive set of interrelated components:
  - Frogans address pattern
  - Frogans address registry
  - Frogans address resolution
  - Frogans address settings
  - Frogans site format
- This security model was developed by taking into account the extensive work carried out by the Internet community to improve domain names (e.g. IDNs) and the DNS (e.g. DNSSEC, NSEC, DANE)

A new security model for online publishing

At a glance (1/2)

Frogans address pattern

Network-name*Site-name

- two-level name space
- asterisk separator character, no dots
- native Unicode support, incl. RTL
- security rules (IETF, Unicode Cons.)
- IFAP specification

Frogans address registry

Frogans Core Registry (FCR)

- delegated to entity (FCR Operator)
- reg. via FCR account administrators using FCR API/HTML interface
- "first-come, first-served"
  - UDRP-F (FORUM and ADNDRC)
- Ten linguistic categories
- employable characters and composition rules at reg. time to mitigate risks of confusion by end users
- FACR specification

Frogans address resolution

Frogans Network System (FNS)

- resolution by FCR Operator
- FNS servers deployed worldwide
- IPv4 and IPv6
- domain names rely on the .frogans TLD
- FNS records signed on the fly (Ed25519)
- authenticated denial of existence
- FNSL specification

At a glance (2/2)

Frogans address settings

- FNS records contain administrative and technical information on the Frogans site
- this information is set by the Frogans address holder and is stored in the FCR
- intended audience managed before the end user accesses to the Frogans site content
- publisher has precise control over the network protocol to be used, incl. TLS cipher suite, SHA512 hash of the SSL certificate, etc.
- no need for Frogans Player to recover from developer's error

Frogans site format

- FSDL is a descriptive language (no scripting)
- based on XML
- FSDL docs and auxiliary files hosted in a single directory on the publisher's server (can be static or generated dynamically)
- FSDL released in the form of an open standard
- Frogans sites offer a complementary and visual way to publish and browse content
- rendered identically on all end-user devices

Frogans address pattern (1/2)

- String of characters used to identify a Frogans site
- Name space has only two levels separated by the asterisk character "*":
  - first level is a network name that designates the Frogans network, i.e. the group that the Frogans site belongs to
  - second level is a site name that reflects the content of that Frogans site
- Frogans address format is: Network-Name*Site-Name
- Length of the network name and site name each limited to between 1 and 28 characters

Frogans address pattern (2/2)

- Can contain international characters (Unicode)
- Can be written from left to right, or from right to left
- Frogans addresses cannot contain the dot character "."
- Eligible characters based on work by the Unicode Consortium and the IETF concerning the use of identifiers and the introduction of IDNs
- Pattern fully described in the International Frogans Address Pattern (IFAP) technical specification https://www.frogans.org/en/resources/ifap/access.html

Frogans address registry (1/4)

- Frogans addresses registered in a central database, called the Frogans Core Registry or FCR
- Database belongs to the OP3FT
- Technical and commercial operation of this database delegated to an entity called the FCR Operator (STG Interactive)
- FCR Operator puts itself at the service of Internet users, in a manner comparable to registry operators for domain names on the Internet
- Registrations made via entities called FCR account administrators using the FCR API or an HTML interface

Frogans address registry (2/4)

- Registrations made using the "first-come, first-served" principle
- Dispute resolution services provided by FORUM and Asian Domain Name Dispute Resolution Centre (ADNDRC) under UDRP-F (adaptation of UDRP to Frogans addresses)
- FCR Operator registration services (Whois, public data, FCR API, HTML interface) accessible over TLS using a second-level domain name of the .frogans TLD : https://fcr.frogans/

Frogans address registry (3/4)

- Employable characters and composition rules are defined to mitigate risks of confusion for end users
- They are enforced by FCR Operator at registration time
- They take into account and combine the outcome of various works concerning international identifiers contributed previously to the community by the Unicode Consortium, the IETF, ICANN, and various domain name registry operators
- They are fully described in the Frogans Address Composition Rules (FACR) technical specification https://www.frogans.org/en/resources/facr/access.html

Frogans address registry (4/4)

- Ten linguistic categories are defined by FACR: LC-Latin, LC-Chinese, LC-Japanese, LC-Korean, LC-Arabic, LC-Cyrillic, LC-Hebrew, LC-Devanagari, LC-Thai, and LC-Greek
- Frogans addresses can be registered in 170+ languages
- Three types of Frogans networks can be used:
  - Public Frogans networks, where the network name is ‘frogans’ or a transcription
  - Dedicated Frogans networks, where the network name is customized
  - Internal Frogans networks (for intranets)

Frogans address resolution (1/3)

- Frogans addresses resolved every time an end user opens a Frogans site (using Frogans Player)
- In addition to operating the FCR, the FCR Operator also proceeds to the resolution of the Frogans addresses of the public and dedicated Frogans networks
- To resolve Frogans addresses, the FCR Operator operates a worldwide infrastructure called the Frogans Network System made up of FNS servers:
  - located in 6 data centers in the US and Europe
  - more to be deployed in Russia and China by end 2017

Frogans address resolution (2/3)

- FNS servers connected to the Internet backbone
- FNS servers run IPv4 and IPv6
- Domain names of FNS servers rely on the .frogans TLD
- Sample domain name of an FNS server:
  fra-par-th2-fns-01-srv-01-01.fns.fcr.frogans
- FNS queried over HTTP 1.1
  (using UCSR network “IP_DNS_TCP_HTTP”)
- FNS servers deliver FNS records

Frogans address resolution (3/3)

- Each FNS record is an XML-based document that complies with the Frogans Network System Language (FNSL) technical specification https://www.frogans.org/en/resources/fnsl/access.html
- FNS records digitally signed on the fly by FNS servers using Ed25519 (as of FNSL 4.0)
- Frogans address resolution ensures authenticated denial of existence
- DDoS protection systems currently being tested
- Frogans addresses of an internal Frogans network are resolved privately on the intranet

Frogans address settings (1/2)

- Each FNS record corresponding to a Frogans address holds the settings of that Frogans address:
  - administrative information such as the intended audience of the Frogans site (age category, countries)
  - technical information on the location of the server hosting the Frogans site and on the network protocols to be used to access the Frogans site (UCSR paths)
  - technical information on the content of the Frogans site (FSDL version used for development, FSDL document encoding, home slide file)
- Frogans address settings are defined by the Frogans address holder and are stored in the FCR

Frogans address settings (2/2)

- Frogans address settings are retrieved prior to accessing the Frogans site, which provides many benefits:
- Administrative information is managed before the end user accesses the content of the Frogans site
- The publisher has precise control over the network protocols to be used for accessing its Frogans site. For example, when using the UCSR network “IP_DNS_TCP_TLS_HTTP”, the UCSR path includes the TLS cipher suite and the SHA512 hash of the SSL certificate, which are verified during the TLS handshake
- Having technical information on the Frogans site content eliminates the need for Frogans Player to guess the developer's intentions or recover from developer’s errors

Frogans site format (1/3)

- Frogans sites are developed using the Frogans Slide Description Language (FSDL)
- FSDL is a description language and not a programming language (there is no scripting on the client side)
- FSDL is based on XML and can be easily hand-coded, using a basic text editor
- All the FSDL documents and auxiliary files of a given Frogans site are hosted in a single directory (the Frogans site root directory) on the publisher's server. They can be static or generated dynamically on the server
- The FSDL technical specification is released in the form of an open standard for the Internet https://www.frogans.org/en/resources/fsdl/access.html

A new security model for online publishing

Frogans site format (2/3)

Frogans site format (3/3)

- Frogans sites are by design smaller, faster to load and more secure than traditional Web sites
- They offer a complementary and highly visual way to publish and browse content online
- They can be published by anyone – from individuals to businesses – and in any language
- Frogans slides are rendered identically by Frogans Player on all end-user devices regardless of the screen size

Further information

- Official Web site of Frogans technology: https://www.frogans.org/
- Addressing services provided by the FCR Operator: https://fcr.frogans/
- Case study on the .frogans TLD published by ICANN: https://newgtlds.icann.org/en/announcements-and-media/case-studies/frogans-a4-26jan17-en.pdf
- Try FSDL using Frogans Player for developers: https://get.frogans/